Opinnäytetyö (AMK)

Tietotekniikka

Hyvinvointiteknologia

2016

Roosa Malinen

TIEDON SIIRTÄMINEN TIETOTURVALLISESTI LÄÄKINNÄLLISESTÄ LAITTEESTA PILVESSÄ OLEVAAN PALVELUUN

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietotekniikka | Hyvinvointiteknologia

2016 | 47

Teppo Saarenpää

Roosa Malinen

TIEDON SIIRTÄMINEN TIETOTURVALLISESTI LÄÄKINNÄLLISESTÄ LAITTEESTA PILVESSÄ OLEVAAN PALVELUUN

Tämän opinnäytetyön tarkoituksena oli tutkia pilvipalveluiden turvallista käyttöä sekä tiedon turvallista siirtämistä pilvessä oleviin palveluihin. Työssä hyödynnettiin erilaisia tietoturvaan liittyviä standardointeja ja ohjeistuksia. Pilvipalveluiden käytön yleistyessä myös palveluiden tietoturvaan tulee kiinnittää entistä enemmän huomiota. Opinnäytetyössä tutkitaan pilvipalveluiden arkkitehtuuria ja palvelumalleja sekä perehdytään tietoturvavaatimuksiin hyödyntämällä KATAKRIA. Tutkimuksessa tutustutaan yleisimmin käytettyihin salausmenetelmiin, kuten RSA ja AES.

Työssä tarkastellaan miten tietoa tulee käsitellä, kuinka palveluun tunnistaudutaan ja tietoaineistoa kontrolloidaan. Kun arkaluontoista tietoa siirretään pilvessä oleviin palveluihin, tulee toimijan huomioida palvelun käyttöönotossa tietosuojavaatimukset tarkasti ja rakentaa palvelun arkkitehtuuri vaatimusten mukaisesti. Tutkimus on jaettu kahteen eri kokonaisuuteen: pilvipalveluihin ja tietoturvaan.

Opinnäytetyö toteutettiin uusimpien standardien ja Suomen lainsäädännön mukaan. Valmista materiaalia potilastietojen siirtämisestä pilvessä oleviin palveluihin ei ollut saatavilla, joten tutkimuksen arkkitehtuuri täytyi rakentaa käytössä olevien menetelmien päälle niin, että ratkaisusta tulisi tietoturvallinen.

Tutkimuksen tuloksena syntyneestä ohjeistuksesta on hyötyä organisaatioille, jotka siirtyvät käyttämään pilvipalveluita sekä haluavat kehittää tiedon suojaukseen liittyvää vaatimustasoa. Tutkimus tarjoaa organisaatiolle arkkitehtuurimalleja palveluiden hankintaan, tietoaineiston salaukseen sekä kontrollointiin.

ASIASANAT:

pilvipalvelut, IaaS, SaaS, PaaS, tietoturva, RSA, AES, tietosuoja, SSL, TLS, OSI, SOA, HIPAA, KATAKRI.

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology | Health Informatics

2016 | 47

Teppo Saarenpää

Roosa Malinen

SECURITY OF DATA TRANSFER FROM MEDICAL DEVICES TO CLOUD SERVICE

The aim of this thesis was to research cloud services security and safe data transfer to cloud services. This thesis utilize different security standards and definitions. Because cloud service usage is becoming more common there is a need to pay attention to service security. In this thesis research concerns architecture of cloud services, service models and security requirements utilizing KATAKRI. In the research introduce general information about encryption methods like RSA and AES.

This research is going to give comprehensive picture about data handling, authentication and controlling data. When transmitting sensitive data to the cloud there is need to consider data protection requirements and architecture requirements when building service. Research is divided on two different parts cloud services and security.

The thesis is implemented with newest standards and Finnish legislation. There was no existing material available about transferring patient data to cloud so the architecture was built on existing solutions in order to create a secure process for the data transmission.

The results of the research are beneficial to organizations that are going to use cloud services and develop their data security. Research offers architecture models for organizations to acquisition services, data encryption and data controlling.

KEYWORDS:

Cloud services, IaaS, SaaS, PaaS, Security, RSA, AES, Data protection, SSL, TLS, OSI, SOA, HIPAA, KATAKRI.

SISÄLTÖ

KUVAT

TAULUKOT

LYHENTEET

AES	kehittynyt lohkosalausjärjestelmä, Advanced Encryption Standard
API	ohjelmointirajapinta, Application Programming Interface
ASCII	7-bittinen tietokoneiden merkistökieli, American Standard Code for Information Interchange
CHAP	salattu tiedonsiirtoprotokolla, Challenge Handshake Authentication Protocol
CRL	sulkulista, Certificate Revocation List
CSA	kanadalainen standardointijärjestö, Canadian Standards Association
CSA	pilvipalveluiden turvallisuutta ohjeistava järjestö, Cloud Security Alliance
DES	salaus protokolla, joka on AES-salauksen edeltäjä, Data Encryption Standard
EAP	tunnistautumisessa käytettävä protokolla, Extensible Authentication Protocol
FIPS	yhdysvaltalainen tietoturvastandardi, Federal Information Processing Standards
FTP	salaamattoman tiedon tiedonsiirtomenetelmä, File Transfer Protocol
GDPR	yleinen tiedon suojaamiseen käytettävä säädös, General Data Protection Regulation.
HetiL	henkilötietolaki 22.4.1999/523
HIPAA	Amerikan yhdysvaltojen terveysvakuutuksen siirrettävyys- ja vastuullisuuslaki, United States Health Insurance Portability and Accountability Act
HITECH	terveysteknologian standardimalli, Health Information Technology for Economic and Clinical Health Act
HTTP	yleinen protokolla tiedonsiirtoon, Hypertext Transfer Protocol
HTTPS	yleinen protokolla salattuun tiedonsiirtoon, Hypertext Transfer Protocol Secure
IaaS	palvelimien ja palvelinsalien ulkoistaminen palveluksi, Infrastructure as a Service
IAM	pääsynhallintamenetelmä, Identity Access Management

IBM	yhdysvaltalainen teknologiayritys, International Business Machines
ICMP	verkkokerroksen protokolla, Internet Control Message Protocol
IP	yleinen verkkokerroksen protokolla, Internet Protocol
ITIL	prosessien hallintaan ja -johtamiseen käytettävä viitekehys, Information Technology Infrastructure Library
ITU	kansainvälinen televiestintäliitto, International Telecommunication Union
KATAKRI	kansallinen turvallisuusauditointikriteeristö
LaaS	koneoppiminen palveluna, Learning as a Service
LADP	tiedon siirtämiseen käytettävä protokolla, Link Access Procedures on the D-channel
MIT	teknillinen korkeakoulu, Massachusetts Institute of Technology
NIST	yhdysvaltalainen mittaustekniikkaa, teknologiaa ja standardeja kehittävä virasto, US National Institute of Standards and Technology
OASIS	kansainvälinen standardointijärjestö IT-alan standardien kehittämiseen, Organization for the Advancement of Structured Information Standards
OCF	avoin viitekehys tietoturva rakenteeseen, Open Certified Framework
OSI	pilviarkkitehtuurien referenssimalli, Open Systems Interconnection reference model
OWL	standardi ontologioiden kuvaamiseen, Web Ontology Language
PAP	tunnistautumisessa käytettävä protokolla, Password Authentication Protocol
PEAP	tunnistautumisessa käytettävä salausprotokolla, Protected Extensible Authentication Protocol
PGP	tietojen salausprotokolla, Pretty Good Privacy
RAMP	referenssiarkkitehtuuri lääkinnällisille komponenteille ja palveluille, Industrial Internet Reference Architecture for Medical Platforms
RBAC	roolipohjainen pääsynhallintamenetelmä, Role Based Access control

RSA	julkisiin avaimiin pohjautuva epäsymmetrinen salausjärjestelmä
SaaS	ohjelmiston hankkiminen palveluna, Software as a Service
SOA	palvelukeskeinen arkkitehtuuri, Service Oriented Architecture
SOAP	tietoliikenneprotokolla, Simple Object Access Protocol
SOCKS	tietoliikenne protokolla pakettien vaihtamiseen, Socket Secure
SSH	salattu tietoliikenneprotokolla, Secure Shell
SSL	tietoliikenneprotokolla, Secure Socket Layer
STAR	rekisteri pilvipalveluiden tietoturvallisuuden tarkastamiseen, Security Trust Assurance Registry
TCG	yhdysvaltalainen tietoturva standardointi järjestö, Trusted Computing Group
TCP	tilallinen protokolla, Transmission Control Protocol
TCCP	tietoturvamalli, Trusted Cloud Computing Platform
TEKES	Teknologian ja Innovaatioiden Kehittämiskeskus
TLS	uudempi versio SSL-salausprotokollasta, Transport Layer Security
TPM	standardi turvalliselle salaussuorittimelle, Trusted Platform Module
UDP	tilaton protokolla, User Datagram Protocol
VALTORI	Valtion tieto- ja viestintätekniikkakeskus
VPN	virtuaalinen erillisverkko, Virtual Private Network
WWW	verkossa toimiva hypertekstijärjestelmä, World Wide Web
W3C	kansainvälinen www-standardien ylläpito- ja kehitysorganisaatio, World Wide Web Consortium
XML	tiedonvälityksessä käytettävä merkintäkieli, Extensible Markup Language

1 JOHDANTO

Tämän opinnäytetyön aiheena on tiedon siirtäminen sairaalaympäristössä olevista lääkinnällisistä laitteista pilvipalveluihin turvallisesti. Työssä tutkitaan pilvipalveluiden ominaisuuksia sekä palveluiden käyttöönotossa huomioitavia mahdollisuuksia ja riskejä. Pilvipalveluiden helppo saatavuus ja käytettävyys ovat potentiaalisia syitä, miksi tietoa halutaan varastoida pilveen. Pilvipalveluiden käyttöönotto on kuitenkin haastavaa, sillä tarjolla olevien palveluiden tietoturvallisuudesta ei ole kunnollisia ohjeistuksia. Potilastietoja siirrettäessä pilvipalveluihin tietoturvalla on merkittävä rooli tietoa käsiteltäessä ja tallennettaessa.

Potilastietojen käsitteleminen Suomessa on säädelty henkilötietolailla sekä yksityisyyden suojaa koskevilla säädöksillä. Sairaalaympäristössä tietoa käsitellään ohjeistuksien ja lakien asettaminen vaatimusten mukaisesti. Arkaluontoisten tietojen käsittelyssä tietoja käsitellään samoja vaatimuksia noudattamalla, ohjelmiston tai lääkinnällisen laitteen alustasta riippumatta. Kun lääkinnällisestä laitteesta siirretään tietoja pilvipalveluihin, tulee palveluissa huomioida tietoturvallisuus erillisenä prosessina projektin läpiviennissä.

Opinnäytetyö esittelee pilvipalveluteknologiaa sekä arkkitehtuurimalleja. Pilvipalveluiden arkkitehtuurimalleissa tutkitaan OSI-referenssimallia (Open Systems Interconnection) ja SOA-referenssimallia (Service Oriented Architecture) sekä niiden hyödyntämistä pilvipalvelua arkkitehtuurissa. Työssä perehdytään lisäksi pilvipalvelumalleihin sekä pilvipalveluiden käyttöönottomalleihin.

Työn laajin osuus koostuu tietosuojasta ja siihen kuuluvasta lainsäädännöstä ja standardeista. Lisäksi tutustutaan tyypillisimpiin tietoturvauhkiin sairaalaympäristössä. Palveluntarjoajilla on nykyään paljon erilaisia vaihtoehtoja pilvipalveluiden toteuttamiseen. Heillä on myös tietoturvaan liittyviä lisäpalveluita, joita kannattaa hyödyntää omassa palvelussa. Työssä kuvataan yleisimpiä tietoturvaratkaisuja ja tietoturvamalleja, joita organisaation on helppo lähteä hyödyntämään omassa palvelussaan.

Opinnäytetyö toteutetaan Innovaatiorahoituskeskuksen Tekesin tukemaan RAMP-projektiin (Industrial Internet Reference Architecture for Medical Platforms). Opinnäytetyön toimeksiantajana on Turun ammattikorkeakoulun tutkimusvastaava Jarkko Paavola.

2 PILVITEKNOLOGIA

Pilviteknologia tarkoittaa tietotekniikan eli laskennan kehitystä ja käyttöä internetissä. Se on uusi menetelmä palveluiden tuottamisessa, käyttämisessä ja toimittamisessa. Pilvilaskenta on toimintamalli, joka mahdollistaa pääsyn skaalautuviin ja vapaasti konfiguroitaviin tietoteknisiin resursseihin. Pilvilaskennan määritelmä perustuu NISTin (US National Institute of Standards and Technology) julkaisuun. (NIST 2016.)

Pilvipalvelut ovat pilvessä eli Internetissä tarjottavia palveluita, jotka jaetaan kolmeen pääluokkaan SaaS (Software as a Service), PaaS (Platform as a Service) ja IaaS (Infrastructure as a Service) (NIST 2011, 2–3). Pilvipalvelut toteutetaan pääasiassa käyttäen ohjelmointirajapintaa API (Application Programming Interface), jossa ohjelmat voivat keskustella vaihtamalla tietoja ja tekemällä pyyntöjä. Ohjelmointikielestä riippuen ohjelmointirajapinnassa suositellaan käytettäväksi XML-merkintäkieltä (Extensible Markup Language) tai SOAP-protokollaa (Simple Object Access Protocol). (Authorize.Net 2015, 8.)

2.1 Pilvipalveluiden ominaisuudet

Pilvipalvelut määritellään erilaisten ominaisuuksien perusteella pilvilaskentaan kuuluviksi. Ensimmäinen ominaisuus on elastisuus, jonka avulla palvelu skaalautuu asiakkaan tarpeisiin sopivaksi ja palvelun kapasiteetin kasvattaminen on helppoa. Toinen ominaisuus on resurssivaranto, jossa palvelun suorittamisessa käytettävillä laitteistoresursseilla on useamman käyttäjän palvelut. Varannon avulla on helppo pitää palveluita yllä, sillä omat fyysiset ympäristöt vaativat enemmän resursseja. Kolmas ominaisuus on riippumattomuus päätelaitteesta ja käyttöpaikasta, jolloin palveluiden käyttö on joustavaa ja monipuolista. (Heino 2010, 48; NIST 2011, 2.)

Pilvipalveluiden neljäs ominaisuus on itsenäisyys, jossa käyttäjät voivat kontrolloida palvelun käyttöä luopumalla palvelusta tai ottamalla palvelun käyttöönsä. Viides ominaisuus on toiminnan mittaus, jossa pilvipalveluiden toimintaa mitataan laskutuksen perusteeksi, sillä asiakkaalle ei koidu fyysisiä laitekustannuksia. (Heino 2010, 48; NIST 2011, 2.)

2.2 Pilvipalvelutyypit

Pilvipalvelut määritetään pilvityyppeihin sen mukaan, kuinka tietoaineistoa kontrolloidaan. Pilvipalvelutyypit voidaan jakaa useampaan luokkaan, joita ovat laskentapilvet, sovelluspilvet, tietovarastopilvet, koneoppiminen, hallinta- ja kehitystyökalut sekä identiteetin ja turvallisuuden hallinta. Luokat voidaan jakaa vielä palveluarkkitehtuurin osiin, joita ovat tallennustila palveluna, tietoturvapalvelut palveluna ja viestintäpalvelut palveluna. Kaikilla pilvipalvelutyypeillä on yhteiset ominaispiirteet, joten palvelut skaalautuvat yrityksen tarpeisiin kattaen perustason teknologian pilvipalvelutyypistä riippumatta. (Salo 2012, 12; Seppälä 2011, 10.)

Laskentapilvi luokitellaan palveluksi, jossa laskentatehoa vuokrataan suurien tietomäärien käsittelemiseen. Virtuaalipalvelimet mahdollistavat tiedon käsittelemisen nopeasti ja tehokkaasti. Laskentapilven teho perustuu pilviverkoissa olevien hajautettujen tietokoneiden laskentakapasiteettiin. Palvelut pohjautuvat IaaS-malliin, jonka etuna ovat palvelinresurssit ja skaalautuvuus. (Seppälä 2011, 10–11.) Amazon, Microsoft, Google ja IBM ovat suurimmat pilvipalveluiden palveluntarjoajat.

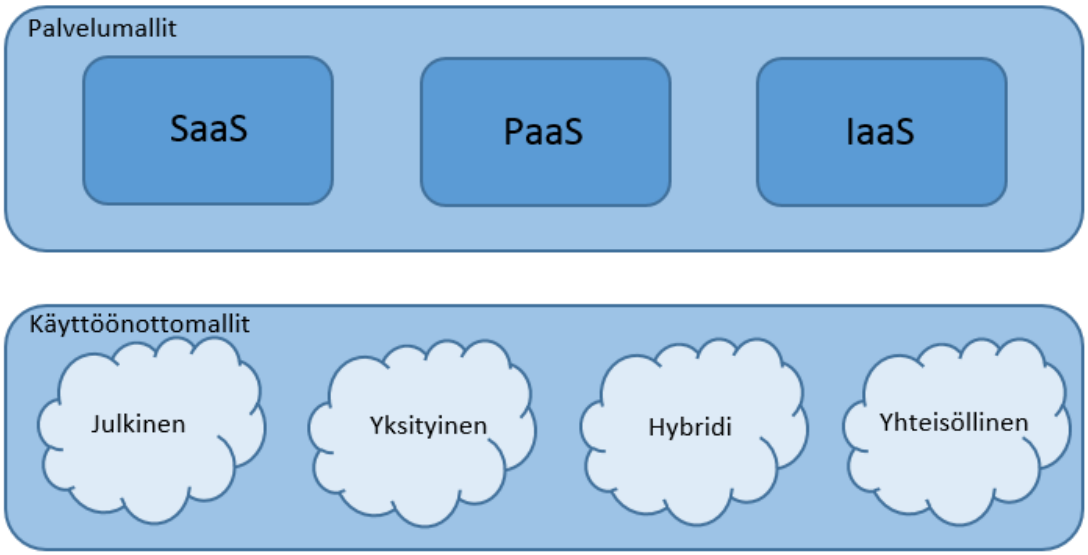
Sovelluspilvipalvelussa asiakas vuokraa sovellusta virtuaalipalvelimilta. Palvelut pohjautuvat SaaS- ja PaaS-malleihin, jotka toimivat IaaSin päällä. Sovelluspilvi tarjoaa asiakkaalle helpon tavan päivittää ja jakaa sovelluksia sekä hallita sovelluslisenssejä.

Tietovarastopilvipalveluissa (Big Data) virtuaalipalvelimelta vuokrataan tallennustilaa asiakkaan tarpeisiin. Palvelut pohjautuvat IaaS-malliin ja palvelua tarjoavat sadat organisaatiot maailmanlaajuisesti (Seppälä 2011, 11). Koneoppiminen palveluna (LaaS) tarjoaa asiakkaalleen mahdollisuuden hyödyntää valtaviakin tietomääriä. LaaS eli Learning as a Service tarjoaa mahdollisuuden muun muassa markkinoinnin kohdentamiseen, asiakaskannan ryhmittelyyn, laitteistojen lokien tarkkailuun ja kannattavuuden ennakointiin. (Google 2016.)

Markkinoilla on saatavilla erilaisia hallintatyökaluja, joita voidaan hyödyntää esimerkiksi monitoroinnissa, virheilmoituksien raportoinnissa sekä pilvipalveluiden resursoinnissa. Saatavilla on myös kehitystyökaluja, joita voidaan käyttää palveluiden rakentamisessa ja tuotannossa. Identiteetin ja turvallisuuden hallintaan käytettävät menetelmät sekä työkalut tukevat tietoturvallisuuden pääsynhallintaa, haavoittuvuuksien tutkimista, palveluiden käytön kontrollointia sekä palveluiden näkyvyyttä. (Google 2016.)

2.3 Pilvipalveluarkkitehtuurit

Pilvipalveluarkkitehtuurin keskeisimmässä osassa ovat Internetistä saatavat palvelut, joita voidaan kutsua avoimen tiedon arkkitehtuuriksi. Pilvipalvelut jaetaan kolmeen palvelukerrokseen, jotka tukevat liiketoimintaprosesseja. Palvelukerrosten kokonaisuutta kutsutaan pilven referenssimalliksi (Kuva 1.), johon kuuluvat sovellukset palveluna (SaaS), sovellusalusta palveluna (PaaS) ja infrastruktuuri palveluna (IaaS). Pilviarkkitehtuuria kuvataan referenssimallin avulla, jotta turvallisuusriskien ymmärtäminen olisi helpompaa. Referenssimallissa ovat kuvattuna pilvipalveluiden käyttöönottomallit, joita ovat yksityinen ja julkinen pilvi, yhteisöllinen pilvi ja hybridipilvi.



Kuva 1. Pilvipalveluarkkitehtuurin referenssimalli.

2.3.1 Sovellukset palveluna (SaaS)

SaaS tarkoittaa ohjelmistojen hankkimista palveluna, jolloin asiakkaan on mahdollista käyttää sovellusta millä tahansa päätelaitteella, myös ilman Internetiä, eikä asiakkaan tarvitse vastata palvelun ylläpidosta. Palvelu kattaa koko infrastruktuurin, johon kuuluu verkot, palvelimet, käyttöjärjestelmät sekä tietokannat. (Salo 2012, 10–17.)

Palvelu veloitetaan lisenssiperusteisesti, jolloin asiakas maksaa vain käytöstä. Palvelu tukee useaa käyttäjää sekä asiakasta samaan aikaan, jolloin resurssien käyttö on tehokasta. SaaS palveluita käytetään Web-selaimessa, erillisesti asennetussa sovelluksessa. SaaS palvelulla voidaan tehostaa työpöytäsovelluksen toimintaa. Sovellukset palveluna ovat markkinoiltaan suurimmat ja pisimmälle kehittyneimmät. (Salo 2012, 10–17.)

2.3.2 Sovellusalusta palveluna (PaaS)

PaaS tarjoaa alustan, jonka päällä sovelluksia voidaan ajaa, testata, ylläpitää ja kehittää. Sovellusalusta palveluna tarjoaa merkittävän hyödyn kehitystyöhön, sillä toiminnollisuudet ja maksulliset lisäosat ovat saatavilla helposti. Kehitystyössä yrityksellä on mahdollisuus kehittää sovelluksiaan kustannustehokkaasti, nopeasti ja tietoturvallisesti. Osaamisvaatimukset asettavat haasteita yritykselle palvelun ollessa uusi ja standardoimaton. (Salo 2012, 10–17.)

Palvelutarjoajan vastuulla on alustan ylläpito ja päivitykset. Myös palvelun toimintavarmuus sekä skaalautuvuus kuuluvat palvelutarjoajan vastuualueisiin. Koodin tuottaminen kuuluu palveluita käyttävän yrityksen vastuulle. PaaS on markkinoiltaan vielä pieni, mutta tarjoaa tulevaisuudessa innovatiivisen kehitysympäristön sovelluskehitykselle. (Salo 2012, 10–17.)

2.3.3 Infrastruktuuri palveluna (IaaS)

IaaS sisältää samat palvelut kuin konesali, mutta palvelut ovat rakennettu virtuaalisesti pilvipalveluun. Infrastruktuuri palveluna kattavat verkkoyhteydet, palvelimet, tallennustilan ja ylläpidon. Asiakas perustaa käyttöjärjestelmän ja sovellukset sekä ostaa laitteiston resurssit käyttöönsä palveluna, jolloin palvelimien hallinta on nopeampaa ja helpompaa. Toimittaja voi myös ylläpitää asiakkaan käyttöjärjestelmää. Palvelun käyttöä laskutetaan käytettyjen tai kiinteiden resurssien perusteella. Palvelun käyttöönotto voi tapahtua itsepalveluna, jolloin vuorovaikutusta ei synny asiakkaan ja palveluntarjoajan välille, tai toimittajan kanssa yhdessä. (Salo 2012, 14.)

IaaS tarjoaa parhaimman liikkumavapauden pilvipalvelumalleista, jolloin asiakkaan on helppo mukauttaa palveluita tarpeidensa mukaan. Haasteena palvelun käytössä on se

että asiakas vastaa itse sovellustensa toimivuudesta, päivityksistä ja tietoturvasta. Palveluita rajoittaa se, ettei asiakas pääse näkemään fyysisiä resursseja. Yleensä asiakkaat kuitenkin tietävät missä palvelimet sijaitsevat. IaaS:iin liittyvät API-rajapinnat sekä tietovarannot ovat usein palvelukohtaisia. (Salo 2012, 14.) Yhdysvaltalainen verkkokauppa Amazon, Microsoft ja Google ovat suurimpia yrityksiä, jotka tarjoavat IaaS-palveluita.

2.3.4 Käyttöönottomallit

Pilvipalvelujen käyttöönottomallit voidaan jakaa neljään ryhmään, joita ovat yksityinen ja julkinen pilvi, yhteisöllinen pilvi ja hybridipilvi. Yksityinen pilvipalvelu toimii yksityisessä lähiverkossa ja palvelu ei tarvitse Internet-yhteyttä palvelun käyttämiseen. Julkista pilvipalvelua käytetään Internetissä päätelaitteen avulla. Yksityiset sekä julkiset pilvet voivat hyödyntää TLS-protokollaa (Transport Layer Security) tietoliikenteen salaamiseen. Julkisen palvelun tietoliikenne voidaan salata myös käyttäen SSH-verkkoliikenneprotokollaa (Secure Shell). Yksityisessä ja julkisessa pilvipalvelussa voidaan myös hyödyntää virtuaalista erillisverkkoa eli VPN-yhteyttä (Virtual Private Network), jolla saadaan yhdistettyä useita verkkoja yhdeksi yksityiseksi verkoksi julkisen verkon yli. Julkinen pilvipalvelu toteutetaan yleensä ympäristössä, jossa palvelut on jaettu useamman käyttäjän kesken. (Heino 2010, 54–56.)

Yhteisöpilvipalvelu on yksityinen pilvipalvelu joka on rajattu eri käyttäjäryhmille. Yhteisöpilvipalvelussa pilveä käyttää useampi käyttäjäryhmä samaan aikaan, jolloin kustannukset jakaantuvat useammalle. Kun yksityinen ja julkinen pilvipalvelu yhdistetään, muodostuu hybridipilvipalvelu. (Salo 2012, 18.) Hybridipilvipalvelu hyödyntää julkisen ja yksityisen pilvipalveluiden ominaisuuksia, jolloin kustannukset ovat alhaiset ja palvelut käytössä tehokkaasti. Palvelumallissa käyttäjällä on käytössään laajemmat palvelut ja käyttäjä pystyy hallinnoimaan resurssejaan paremmin kuin muissa malleissa. (Salo 2012, 16.)

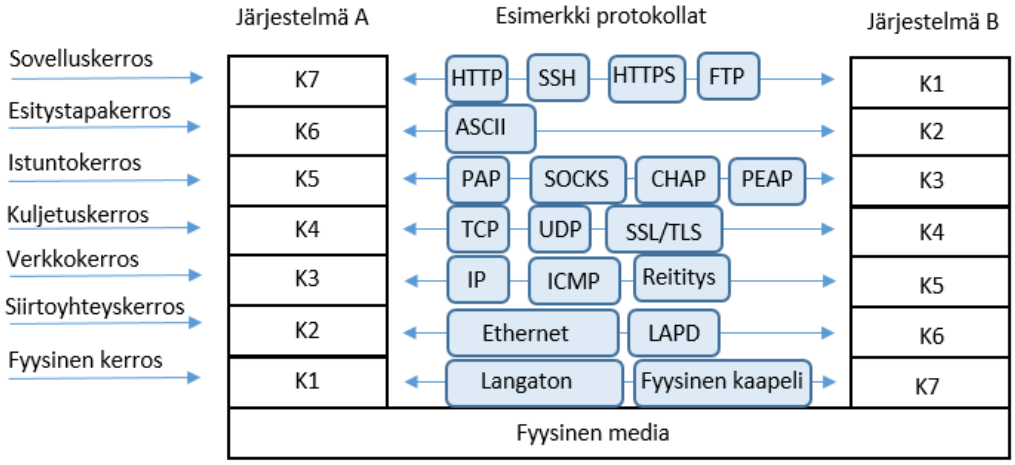
2.3.5 OSI-referenssimalli

Pilvipalveluarkkitehtuuria voidaan kuvata myös OSI-referenssimallin (Open Systems Interconnection Reference Model) avulla. OSI kuvaa tiedonsiirtoprotokollien kerroksien yhdistelmää. OSI-mallissa on seitsemän kerrosta, jotka pohjautuvat ISO 7498 -standardiin.

Standardia käsitellään ITU:n (International Telecommunication Union) dokumentissa (ITU 1994.). OSI-mallin kerrokset näkyvät kuvassa 2.

Kuvan 2 ensimmäinen kerros koostuu fyysisestä kerroksesta, joka määrittelee fyysisen median siirtotien. Fyysinen media voidaan siirtää käyttämällä erilaisia tekniikoita, kuten langatonta tai langallista siirtotietä. Langattomassa siirtotiessä tieto siirtyy ilmassa tai väliaineessa antennien välityksellä. Langallisessa siirtotiessä tieto siirtyy johtimien kautta esimerkiksi optista kuitua käyttäen. Toinen kerros määrittelee kehyksen edeltävälle fyysiselle kerrokselle ja tätä kutsutaan siirtoyhteyskerrokseksi. Siirtoyhteyskerroksessa tapahtuu yhteyden luominen, virheiden korjaaminen sekä yhteyden purkaminen. Siirtoyhteyskerroksen yhteyskäytäntönä voidaan käyttää LADP (Link Access Procedures on the D-channel) protokollaa käyttäjän ja verkon väliseen tiedon siirtoon. (ITU 1994, 46−52.)

Kuvan 2 kolmas kerros käsittelee verkkokerrosta, joka tarjoaa yhteyden molempiin suuntiin. Verkkokerroksen on tarkoitus valita sanomille reitti, jota pitkin sanomat lähetetään. Verkkokerrokseen kuuluva IP-protokolla (Internet Protocol) välittää tietoliikennepaketteja verkon laitteiden välillä. ICMP (Internet Control Message Protocol) toimii verkkokerroksen päällä. ICMP-protokollan avulla reitittimet lähettävät kyselysanoman ja isäntä vastaa ilmoitusanomalla. (ITU 1994, 41−46.)



Kuva 2. OSI-referenssimallin seitsemän kerrosta.

Kuvan 2 neljänteen kerrokseen kuuluu kuljetuskerros, joka pitää huolen siitä, että tieto tulee oikein järjestettynä perille. TCP-kuljetusprotokolla (Transmission Control Protocol) tarjoaa kuljetuksen eri prosessien välille ja muodostaa yhteyden laitteiden välille ennen

tiedon siirtämistä. Kun taas UDP-kuljetusprotokolla (User Datagram Protocol) tarjoaa ainoastaan tiedon kuljetuspalvelun, mutta ei huolehdi kuljetuksen luotettavuudesta, niin kuin TCP-protokolla. Kuljetuskerrokseen kuuluu SSL/TLS-tietoliikenneprotokolla (Secure Socket Layer/Transport Layer Security), jolla suojataan sovellusten tietoliikenne IP-verkkojen yli. (ITU 1994, 37−41.)

Viides kerros (Kuva 2.) kuvaa istuntokerrosta, joka ylläpitää useiden istuntojen kanavoimisen oikein. Istuntokerroksessa käytettäviä protokollia ovat muun muassa PAP-protokolla (Password Authentication Protocol), CHAP-protokolla (Challenge Handshake Authentication Protocol), PEAP-protokolla (Protected Extensible Authentication Protocol) ja SOCKS-protokolla (Socket Secure). PAP on tunnistuksessa käytettävä protokolla. Salasanat sekä käyttäjätunnukset kulkevat selkokielisenä siirtotiellä, joten PAP-protokollaa ei ole turvallista käyttää. (ITU 1994, 34−37.)

CHAP on parempi versio PAP-protokollasta. CHAP-protokollassa tieto kulkee siirtoyhteyskerroksen avulla salattuna. PEAP on suojattu versio EAP-protokollasta (Extensible Authentication Protocol). PEAP tarjoaa kaksivaiheisen tunnistautumismenettelyn, jossa luodaan turvallinen TLS-kanava. Tämän avulla henkilön ei tarvitse paljastaa omaa henkilöllisyyttään tunnistautuessaan palveluun. SOCKS-protokollaa käytetään pakettien vaihtamiseen asiakkaan ja palvelimen välillä välityspalvelimen (Proxy) läpi. (ITU 1994, 34−37.)

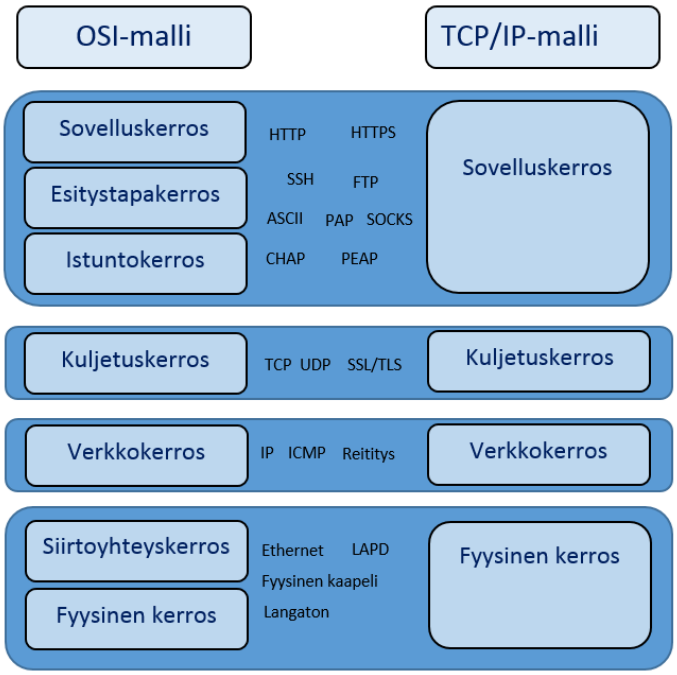
Kuvan 2 kuudes kerros on esitystapakerros, joka vastaa merkistökoodauksen yhteensopivuudesta. Esitystapakerroksen tarkoituksena on päättää missä muodossa tieto näytetään tiedonsiirron yhteydessä. Esitystapakerrokseen kuuluu muun muassa ASCII-merkistö (American Standard Code for Information Interchange). ASCII-merkistöä käytetään tietokoneen merkistökoodaamiseen. (ITU 1994, 33−34.)

Kuvan 2 viimeinen kerros kuvaa sovelluskerrosta, jossa sovellusta käytetään viestintään. Sovelluskerroksen sovellukset näkyvät käyttäjälle Internet-linkistä. Esimerkiksi HTTP (Hypertext Transfer Protocol) tai HTTPS (Hypertext Transfer Protocol Secure) tekevät koodin käyttäjälle näkyväksi. HTTP on protokolla, jota selaimet ja Web-sivut käyttävät tiedonsiirtoon. HTTP-protokollan ja HTTPS-protokollan ero on se, että HTTPS-protokollaa käytetään salattuun tiedonsiirtämiseen. SSH eli Secure Shell on tietoliikenteen salaamiseen käytettävä protokolla. SSH-protokollaa käytetään turvallisen etäyhteyden muodostamiseksi asiakkaan ja palvelimen välillä. Sovelluskerrokseen kuuluu myös FTP-

protokolla (File Transfer Protocol), jota käytetään tiedonsiirtämiseen, ilman tiedon salaamista. (ITU 1994, 32−33.)

2.3.6 TCP/IP-viitemalli

Yleisen arkkitehtuurin kuvaamiseen käytetään myös TCP/IP-viitemallia (Transmission Control Protocol / Internet Protocol), joka on Internetin arkkitehtuurin määrittelemiseen käytettävä protokolla. Toisin kuin OSI-malli TCP/IP-viitemallin käyttö soveltuu vain TCP/IP protokollapinojen mallintamiseen. Kuitenkin viitemallista voidaan nähdä samankaltaisuuksia mallien kerroksissa. TCP/IP koostuu vain neljästä portaasta, kun taas OSI-mallissa kerrokset on jaettu seitsemään osaan. TCP/IP-viitemallin arkkitehtuuri perustuu yhteiseen IP-protokollaan (Internet Protocol), jossa IP-paketteja voidaan lähettää fyysisen kerroksen päältä. TCP/IP-viitemallissa (Kuva 3.) kuvatut neljä kerrosta ovat sovelluskerros, kuljetuskerros, verkkokerros ja fyysinen kerros. (IBM 2006, 3–9.)



Kuva 3. OSI-mallin ja TCP/IP-viitemallin arkkitehtuurit.

Ensimmäinen kerros alkaa sovelluskerroksesta. Sovelluskerroksen tietoliikenne edellyttää yleisesti muiden protokollien käyttöä salattuun liikenteeseen. Yleisin pankkien käyt-

tämä yhteys on salattu HTTP-siirtoprotokolla (Hypertext Transfer Protocol). HTTP-protokolla toteutetaan palvelussa tunneloimalla protokollaa SSL/TLS-protokollan päällä. (IBM 2006, 3–9.)

Mallin toinen kerros kuvaa kuljetuskerrosta. Kuljetuskerros sallii tietoliikenneyhteyden lähteen ja kohteen välille. Kuljetuskerros toimii samankaltaisesti TCP/IP-viitemallissa, kuin OSI-mallissa toteuttaen ruuhkanhallintaa, mikä estää liikenteen ruuhkautumisen ja pakettien toimittamisen siinä järjestyksessä, kun paketit on lähetetty. TCP-protokollan sijasta voidaan käyttää UDP-protokollaa (User Datagram Protocol), joka voi siirtää paketteja tilattomasti laitteiden välillä. Tämä mahdollistaa sen että UDP-protokollalla pakettien käsittelyä voidaan nopeuttaa huomattavasti ja pakettien siirtäminen on helppokäyttöisempää kuin TCP-protokollalla. (IBM 2006, 3–9.)

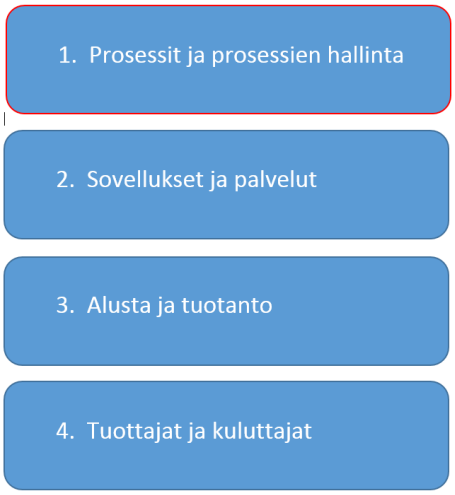
Kolmas porras on verkkokerros, jossa paketit lähetetään verkon tietokoneiden välillä. Reitittimet ottavat paketit vastaan sekä ohjaavat paketit eteenpäin. Viimeinen TCP/IP-viitemallin kerros on fyysinen kerros, jossa määritellään linkkikerroksen tekniikat. IP-tekniikka tarvitsee käyttöönsä alemman portaan palveluita, jotta se voi lähettää paketteja reitittimille. Samoin kuin OSI-mallissa, fyysisessä kerroksessa käytettyjä tekniikoita ovat muun muassa Ethernet-lähiverkko yhteys ja TCP/IP-protokollapino. (IBM 2006, 3–9.)

2.3.7 SOA-arkkitehtuurimalli

Pilvipalveluarkkitehtuurissa voidaan hyödyntää myös palvelukeskeistä arkkitehtuuria SOA (Service Oriented Architecture), jossa tietojärjestelmien prosessit ja toiminnot pyrkivät toimimaan itsenäisesti ja avoimesti. SOA-arkkitehtuurissa palveluita käyttävät toiset sovellukset, hyödyntäen avoimia rajapintoja ja sovelluspalveluiden järjestelmiä. (W3C 2012.)

Palvelukeskeisen arkkitehtuurin rakennetta kuvataan OASIS:in (Organization for the Advancement of Structured Information Standards) dokumentissa (OASIS 2012, 9; OASIS 2016). Mallin tavoitteena on ohjata henkilöitä, jotka tekevät töitä arkkitehtuurin parissa. SOA-viitekehyksen arkkitehtuurissa (Kuva 4.) on kuvattuna prosessit ja niiden hallinta, sovellukset ja palvelut, sekä alusta ja tuotanto. Myös tuottajat ja kuluttajat ovat huomioitu arkkitehtuurimallissa.

On myös tärkeää huomioida, että SOA:n arkkitehtuurimallin prosessit ja niiden hallintaan kuuluvat vaatimukset, motivaatio ja sidosryhmien tavoitteet ovat määritelty kriittisiksi osiksi arkkitehtuurin kokonaisuudessa. (OASIS 2016.)



Kuva 4. Palvelukeskeisen SOA-arkkitehtuurin referenssimalli.

Pilvipalveluarkkitehtuurin suunnittelussa tulee huomioida semanttisen Webin käyttö. Semanttinen Web on WWW-palvelun (World Wide Web) laajennus, jossa tietokone tulkitsee irrallisten sanojen ja linkkien välisen merkityksen, käyttämällä ontologia-pohjaista ohjelmaa, kuten OWL-kuvailukieltä (Web Ontology Language). OWL perustuu W3C:en (World Wide Web Consortium) määrittelemään standardiin tiedon kuvailukielistä. OWL jakaantuu kolmeen kieleen (OWL Lite, OWL DL, OWL full) ja niitä käytetään ohjelmissa kuvaillun tiedon päättelyyn ja tulkintaan. (W3C 2013.)

2.4 Pilvipalveluiden saatavuus

Pilvipalveluiden saatavuus on yksi pilvipalveluiden suurimmista hyödyistä. Palvelut ovat saatavilla kokoajan ja käyttäjä voi määritellä itselleen palvelutason, jossa sovitaan sopimusvelvotteet sekä palveluiden ylläpito. Sopimusvelvotteisiin on hyvä tutustua tarkasti ennen palvelun käyttöönottoa, sillä maksujen myöhästyessä palvelunkäyttö voidaan evätä taikka tiedot poistaa. Palveluita hankittaessa tulee noudattaa EU:n komission hyväksymiä maita, joilla on riittävä tietosuoja, kun henkilötietoja siirretään ulkomaille.

Palveluita on saatavilla kaiken kokoisille organisaatioille, ja lisäpalvelutarjonta on erittäin kattavaa. Pilviteknologiaa tarjoavat useat palveluntarjoajat pienistä yrityksistä maailmanlaajuisiin yrityksiin. Isoimmat yritykset, kuten Google ja Microsoft tarjoavat laajimmat palvelut pilveen. Yrityksien palvelut ovat monessa tapauksessa hajautettu eri palvelimille, jolloin käyttäjien tiedot voivat sijaita globaalisti missä vain. Tiedon hajauttaminen mahdollistaa palvelulle hyvän toimintaympäristön palvelimen kaatuessa, jos käyttöön on hankittu varakapasiteettia. Näin saadaan minimoitua riskit koko järjestelmän kaatumisesta.

3 PILVIPALVELUIDEN TIETOTURVA

Yleisesti pilvipalveluiden tietoturvan tavoitteena on varmistaa, että tiedot pysyvät tallessa luottamuksellisena ja eheänä. Pilvipalveluiden tietoturvaan vaikuttavat tekijät eivät näy aina loppukäyttäjälle. Teknisten toteutuksien, kuten ohjelmistojen ja laitteiston lisäksi ympäröivä maailma vaikuttaa palveluiden tietoturvaan. Turvallisuutta arvioitaessa tulee arvioida palveluntarjoajien toimintaa ja palvelun toteutusta. Sertifikaatteihin, auditointeihin, ja palveluntarjoajien dokumentteihin kannattaa kiinnittää huomiota palvelua hankkiessa. (Kyberturvallisuuskeskus 2014, 12; Honkasalo 2014, 10.)

Tiedon omistajuus on määritelty siten, että oikeudet ovat palvelussa tiedon tuottajalla. Lainsäädäntöä noudattamalla oikeudet ja omistajuus voidaan kuitenkin siirtää sopimusten perusteella. Tiedon tuhoaminen vaatii oikeudet järjestelmään, jolloin tiedon poistamiseen tulee määrittää erilliset oikeudet käyttäjälle. Tiedot voivat sijaita yhdessä tai useammassa paikassa omissa konesaleissa tai palvelinkeskuksissa. Resurssit voidaan myös vuokrata ulkoiselta palveluntarjoajalta. Turvallisin tapa on hajauttaa palvelukeskukset niin, että vian ilmetessä palvelu voidaan tarjota toiselta palvelinkeskukselta. (Kyberturvallisuuskeskus 2014, 9.)

Pilvipalveluiden tekniseen tietoturvaan vaikuttavat toimintamallit, käytettävät teknologiat sekä standardit. Ohjelmistojen ja infrastruktuurin päivityskäytännöt on myös hyvä selvittää ennen pilvipalvelun käyttöönottoa. Pilvipalveluissa tieto voi olla tallennettu useaan paikkaan. Tieto on yleensä tallennettu samanaikaisesti järjestelmien muistiin, ulkoiseen massamuistiin tai tietokantaan. Tiedot on aina syytä varmuuskopioida tai vähintään kahdentaa. Kuitenkin palvelun hankinnassa kannattaa ottaa huomioon se, että tiedot voivat korruptoitua, jolloin kahdentamisesta ei ole hyötyä. Tieto voidaan sijoittaa palvelutarjoajien sijaintien mukaan globaalisti. Palvelun hankinnassa täytyy huomioida eriävätkö eri palvelutarjoajien noudattamat lait ja standardit oman maan lainsäädännöstä sekä onko muiden maiden viranomaisilla oikeus päästä tietoihin käsiksi. (Kyberturvallisuuskeskus 2014, 8–12.)

Opinnäytetyössä sovelletaan tietoturvaa hybridipilvipalveluihin, sillä hybridipilvi on ominaisuuksiltaan ja skaalautuvuudeltaan soveltuvin vaihtoehto projektiin. Tietoturvaa käsitellään kuitenkin sellaisella tasolla, että sitä voidaan hyödyntää myös muiden pilvipalveluiden käyttöönottomalleissa.

3.1 Tietosuoja

Tietosuojaa tarkastellaan henkilötietolain näkökulmasta. Tietosuojan tarkoituksena on suojata palvelun käyttäjää. Kun tietoja siirrettään, muokataan, tallennetaan tai käsitellään, vastuu tietojenkäsittelystä on henkilötietolain mukaan tietoja käsittelevällä henkilöllä (HetiL 3 §). Tällöin pilvipalveluiden käyttäjä on vastuussa tiedosta rekisterinpitäjänä ja rekisterin sekä käsittelyn lainmukaisuudesta. Yleensä palveluntarjoaja ei vastaa henkilötietojen käsittelystä. (Suomi 2015.)

Tietojen suojaamisessa rekisterinpitäjän on toteutettava tarvittavat toimenpiteet henkilötietojen suojaamiseen. Toteuttamisessa on otettava huomioon tekniset mahdollisuudet, kustannukset, tiedon laatu, määrä ja ikä, sekä käsittelyn merkitys. Kun pilvipalvelua hankitaan, palveluntarjoajalta on rekisterinpitäjälle annettava selvitykset ja sitoumukset henkilötietojen suojaamisesta. (HetiL 32 §.)

Tietosuojastandardi ISO/IEC 29100 määrittelee tietosuojamallin, jota voidaan soveltaa henkilöihin ja organisaatioihin, jotka käsittelevät henkilötietoja. Palveluiden hankinnassa on hyvä huomata voimaan tullut uusi EU:n tietosuoja asetus, jossa vaatimukset ovat määritelty entistä tarkemmin. Asetuksen tavoitteena on luoda yhtenäisempi ja ajanmukaisempi kehys henkilötietojen käsittelyyn. Asetuksen oletettu voimaantuloaika on vuonna 2018. (Kunnat.net 2016.)

3.2 Lainsäädäntö

Henkilötietolaki on henkilötietojen käsittelyyn tarkoitettu yleislaki. Lakia sovelletaan aina, kun henkilötietoja käsitellään automaation avulla tai muuten (HetiL 2 §). Kun Euroopan unionin ulkopuolella oleva rekisterinpitäjä käyttää henkilötietojen käsittelyssä Suomessa sijaitsevia laitteita muuhunkin tarkoitukseen kuin tiedonsiirtoon, henkilötietolakia sovelletaan henkilötietolain 4 §:n mukaan. Kuitenkin poikkeukset arkaluonteisten tietojen käsittelyssä kattaa terveydenhuollon toimintayksikön tai ammattihenkilön luvan käsitellä potilastietoja (HetiL 12 §). Rekisterinpitäjän on lähetettävä rekisteriseloste tietosuojavaltuutetulle, sekä ilmoitettava jos henkilötietoja siirretään Euroopan unionin ulkopuolelle (HetiL 36 §).

Tietoyhteiskuntakaarta (1.11.2014/917) sovelletaan yhdessä henkilötietolain kanssa. Lain tarkoituksena on turvata luottamuksellisuuden ja yksityisyyden suojan toteutuminen, sekä edistää tietoturvaa ja sähköisten palveluiden kehittymistä. Lakia sovelletaan viestintäverkoissa tarjottaviin palveluihin. (Tietoyhteiskuntakaari 2014.)

Valtioneuvoston asetus (1.7.2010/681) tietoturvallisuudesta valtionhallinnossa säätää tietoturvallisuusvaatimukset asiakirjojen käsittelyyn. Asetuksen turvallisuusvaatimuksia voidaan hyödyntää pilvipalvelun käyttöönotossa huomioitavaan tietoturvan perustason toteuttamiseen 3 §:n mukaan. Palvelun hankinnassa voi käyttää apuna myös 9 §:ssä käsittelyvaatimuksia osoittavia suojaustasoja. (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681.)

3.3 Standardit

Tietoturvanhallinta järjestelmä standardia ISO/IEC 27000 sovelletaan tietoturvallisuuden hallintaan, riskeihin ja kontrollointiin. ISO 27000 standardi perheeseen kuuluu Menettelyohjeet henkilötietojen suojaamiseen henkilötietoja käsittelevissä julkisissa palveluissa SFS-ISO/IEC 27018, jossa esitetään hyväksytyt tavoitteet, keinot ja ohjeet henkilötietojen suojaamiseen pilvipalveluissa. Tietosuojaperiaatteet nojautuvat tietosuojastandardiin ISO/IEC 29100.

ITU määrittelee viitekehyksen pilvipalveluiden tietoturvallisuudelle. Viitekehyksessä kuvataan muun muassa tietoturvauhkien havainnointiin, tiedon katoamiseen tai vuotoon, käyttöoikeuksiin, sisäisiin tietoturvauhkiin, ja luottamuksen puutteeseen liittyviä asioita. ITU noudattaa ISO 27000 standardiperheen lisäksi NIST:in ja CSA:n (Cloud Security Alliance) määrittelemiä tietoturvamalleja ja suosituksia. (ITU 2014.)

ITIL-viitekehys (Information Technology Infrastructure Library) määrittelee prosessimallin muun muassa tietoteknisten palveluiden hallintaan ja johtamiseen. ITIL-viitekehys kattaa prosessien koko elinkaaren ja sitä voidaan soveltaa myös pilvipalveluiden hallinnassa yhdessä NIST:in ja ITSM:in (IT Service Management) määrittelemien viitekehysten kanssa SaaS-palveluita hankittaessa. (ITIL 2014, 3–13.)

Monet uusimmat palvelut käyttävät KATAKRI (Kansallinen turvallisuusauditointikriteeristö), VAHTI (Valtionhallinnon tietoturvallisuuden johtoryhmä) ja HITECH (Health Information Technology for Economic and Clinical Health Act) tietoturvastandardointeja. KATAKRI kattaa kolme osa-aluetta, joita ovat turvallisuusjohtaminen, fyysinen turvallisuus

ja tekninen turvallisuus. VAHTI on jaettu kahdeksaan osaan, joita ovat hallinnollinen tietoturva, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus, käyttöturvallisuus ja laitteistoturvallisuus. KATAKRI ja VAHTI noudattavat lähes samanlaisia vaatimuksia tietoturvallisuuden suhteen. HITECH määrittelee salassa pidettävien terveystietojen riittävän hyvän suojaamisen. (KATAKRI 2015, VAHTI 2009, Microsoft 2015.)

3.4 HIPAA

HIPAA (Health Insurance Portability and Accountability Act) on yhdysvaltalainen vuonna 1996 määritelty potilastietojen ja terveystietojen käsittelyä koskeva laki. Lain tarkoituksena on määritellä vaatimukset arkaluontoisen tiedon käytölle, salassapidolle ja julkistamiselle. HIPAA määrittelee vaatimukset henkilöllisyyden tunnistamisen perusteella. Mikäli tiedoista voidaan tunnistaa potilas tietojen käsittelyn vaatimukset noudattavat HIPAA-lakia. Laki on asetettu koskemaan kaikkia, jotka käsittelevät terveystietoja USA:ssa. Laki koskee myös terveydenhuollon muita toimijoita ja palveluita, jotka käsittelevät salassa pidettäviä tietoja. (Microsoft 2015.)

HIPAA voidaan jakaa neljään osaan, jossa määritellään tietosuoja ja potilaan tietojen luottamuksellinen käsittely, fyysinen ja tekninen tietoturva, tunnistetiedot ja tutkimustietojen kerääminen, terveyteen liittyvien sähköisten lähetysten maksut ja kelpoisuus. HIPAA sisältää myös BA-sopimuksen (Business Association), joka määrittelee organisaatiota koskevat vaatimukset. BA-sopimukset rajoittavat liiketoiminnassa käytettäviä tapoja ja selkeyttävät salassa pidettävien tietojen käsittelyä. (Microsoft 2015.)

HIPAA määrittelee terveydenhuollon toimialan tietojärjestelmille vaatimuksia, joissa potilastiedot tulee suojata koko talletusajan. Potilastietojen dokumentointia tulee valvoa keskitetysti. Potilastietoja käsittelevällä toimijalla tulee olla hallinnollinen ja tekninen arkkitehtuuri tietojen luottamuksellisuuden ja muuttumattomuuden varmistamiseen koko tietojen käsittelyyn liittyvän elinkaaren ajan. (Health Insurance Portability and Accountability Act 2016.)

Tietojen käsittelyn tulee olla tarkoin suojattua, jotta arkaluontoinen tieto ei pääse ulkopuolisten käyttöön. HIPAA määrittelee myös organisaation tietojen kontrolloinnin, kuten

pääsynvalvonnan ja identiteetin todennuksen. Potilastiedot tulee olla suojattuna monitasoisesti sekä tiedoista tulee pitää hakemistoa, josta ilmenee asiakirjojen käsittelyyn liittyvä hallinta. (Health Insurance Portability and Accountability Act 2016.)

HIPAA-lakia ei voida kuitenkaan soveltaa täysin sellaisenaan Suomessa, sillä USA:n lainsäädäntö poikkeaa Suomen lainsäädännöstä. HIPAA antaa kuitenkin erittäin hyvän lähestymistavan arkaluontoisten tietojen käsittelyyn ja suojaamiseen.

3.5 GDPR-säädös

Pilvipalveluiden käyttöönotossa olisi hyvä huomioida myös viimeistelevä GDPR-säädös (General Data Protection Regulation). Kuvassa 5 on esitelty 12-portainen ohje yleiseen tiedonsuojaamiseen.

Kuva 5. 12 askelta tiedon suojaamiseen (ICO 2016, 2).

Ensimmäisessä kohdassa ohjataan olemaan tietoisia muuttuvista laeista, säädöksistä ja standardeista. Kohdassa 2 kehotetaan dokumentoimaan kaikki henkilötietojen käsittelyyn liittyvät asiat. Yrityksen täytyy myös pystyä näyttämään miten tietosuojalakia noudatetaan organisaatiossa. (ICO 2016, 5–6) Kolmanteen askeleeseen kuuluu tietosuojasäännösten katselmointi mahdollisilta muutoksilta, tämä kohta eroaa kohdasta 1 siten, että kohdassa 3 määritellään kuinka tiedotetaan henkilöitä, joiden henkilötietoja yritys käsittelee. Neljännessä askelmassa ohjataan tarkistamaan kaikki menettelytavat ja oikeudet, joita yksilöllä on kun tietoja käsitellään toisen osapuolen toimesta. (ICO 2016, 5–6.)

Kohdassa 5 kehotetaan suunnittelemaan tietojen päivittäminen ja ylläpito sekä seuraamaan tietojen päivittämiseen ja ylläpitämiseen liittyviä säädöksiä. Kuudennessa askeleessa ohjataan tarkastelemaan erilaisia tietojenkäsittelytapoja ja malleja noudattamalla samalla säädöksiä ja lakeja. Seitsemännessä kohdassa käsitellään yksilön suostumusten tallentamista, muuttamista ja tulkintaa. Seuraava askel syventää kohdassa 7 mainittuja asioita lasten henkilötietojen käsittelyyn. (ICO 2016, 7–8.)

Kohdassa 8 kiinnitetään huomio lasten tietojenkäsittelyyn vanhempien suostumuksella. Yhdeksännessä askelmassa organisaation tulee varmistaa, että tietojenkäsittelyyn liittyvien rikkomusten tai tietoturvaloukkausten menettelytavat ovat lainmukaiset. Kohdassa 10 opastetaan riskienhallintaan ja projektinhallintaan PIA:n (Privacy Impact Assessments) ohjeistusta hyödyntäen. Portaassa 11 kehotetaan valitsemaan tietosuojavaltuutettu organisaatiolle. Viimeinen porras ohjeistaa kansainvälisen organisaation määrittämään minkä tietosuojaviranomaisen alaisuuteen organisaatio kuuluu. (ICO 2016, 8–11.)

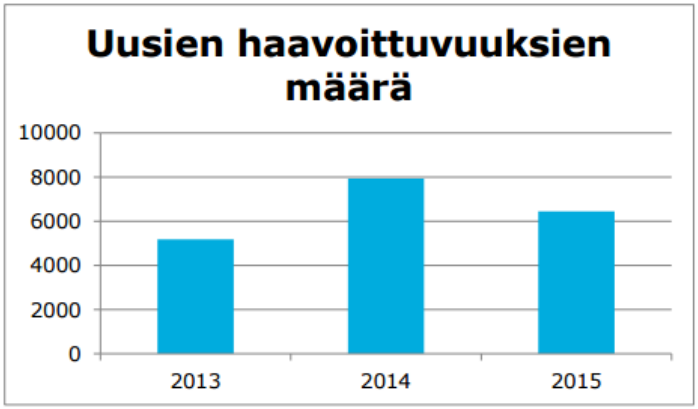
3.6 Tietoturvauhkat

Monet tietoturvauhkat liittyvät terveydenhuollon organisaatiossa lääkinnällisten laitteiden tiedonhallintaan, jossa tiedonhallinta on ylläpidon vastuulla. Lääkinnällisten laiteiden ohjelmistovirheet aiheuttavat haavoittuvuuksia, jolloin komentoja voidaan suorittaa mielivaltaisesti sekä käyttöoikeuksia voidaan laajentaa. Yleisimpiä tietoturvauhkia ovat tiedon luvaton käyttö, salatun tiedon paljastuminen, tiedon kopiointi, muuttaminen tai häviäminen, salassa pidettävän tiedon tutkiminen sekä luvaton käyttö. Ulkoisia tietoturvauhkia

ovat haittaohjelmat, tietovuodot sekä tietomurrot. Myös ihmisten tekemät virheet ja vahingot vaikuttavat tietoturvauhkien lisääntymiseen. Yleisimmät syyt tähän ovat heikot salasanat, konfiguraatiovirheet tai koulutuksen puute. (Viestintävirasto 2016, 3.)

Tyypillisimmät tietoturvauhkat pilvipalveluissa ovat palveluiden käyttöön ja valvontaan liittyvät oikeudet, epäluotettavat palveluidentarjoajat ja yleinen heikko tietoturvallisuus. Monilla palveluntarjoajilla on rajaton pääsy asiakkaan tietoihin, mikä aiheuttaa epävarmuutta tietoturvan suhteen. Lisäksi ohjelmistovirheet sekä järjestelmän kaatuminen voi tuhota tai kadottaa tietoa.

Teknisiin tietoturvauhkiin pilvipalvelussa kuuluu pääsynvalvonnan huono toteuttaminen, käyttöjärjestelmiin, sovelluksiin ja tietokantoihin kohdistuvat hyökkäykset, verkkohyökkäykset, palvelunestohyökkäykset, verkkoväärennökset, huonot tiedon tallennusvälineet, evästeet ja erilaiset haittaohjelmat. Haavoittuvuuksien huono testaaminen on usein syynä sille, että järjestelmiin päästään murtautumaan. Hyökkääjä pystyy hyödyntämään palvelun haavoittuvuuksia ja hyökätä organisaation tai palveluun. Kuitenkin tunnettujen uusien haavoittuvuuksien määrää on saatu laskettua vuodesta 2014. Kuvassa 6 näkyy uusien ohjelmistohaavoittuvuuksien määrä.



Kuva 6. Tunnettujen ohjelmistohaavoittuvuuksien määrä vuosittain (Viestintävirasto 2016, 4).

Pylväät kuvaavat haavoittuvuuksien määrää vuosien 2013, 2014 ja 2015 aikana. Vuonna 2013 haavoittuvuuksien määrä on ollut alimmillaan, mikä voi johtua siitä, että haavoittuvuuksia ei ole pystytty havaitsemaan. Vuonna 2014 haavoittuvuuksien määrä nousi noin 2500:lla, mutta laski sitten noin 2000:lla vuonna 2015. Tämä muutos voi johtua siitä, että haavoittuvuudet huomattiin ja ohjelmistoja alettiin korjaamaan.

Kuvasta 5 voidaan havaita, että haavoittuvuuksien määrä on laskussa, mutta edelleen korkea. Korkea haavoittuvuuksien määrä voi johtua siitä, että haavoittuvuuksista ei olla organisaation sisällä tietoisia. Haavoittuvuuksien määrä voi kuitenkin olla vielä korkeampi, sillä tunnistamattomia haavoittuvuuksia ei ole huomioitu kuvassa 6. Haavoittuvuuksien määrään voi vaikuttaa nostavasti myös se, että ohjelmistoja sekä järjestelmiä on nykyään useita.

3.7 Tietoturvaratkaisut

Erilaisia tietoturvaratkaisuja voidaan soveltaa terveydenhuollon organisaation haavoittuvuuksien hallintakyvyn mukaan. Tietoturvaratkaisuun vaikuttaa ennalta suunniteltu toiminta palvelun hankinnassa, käyttöönotossa, käytössä ja palvelun lopettamisessa. Myös ajantasaisella listalla käytössä olevista laitteista ja niiden ohjelmistoista saadaan minimoitua laitekohtaiset riskit. Laitteiden, järjestelmien, ohjelmistojen sekä sovellusten riippuvuudet tulee arvioida ennakkoon, sekä sovellusten ja laitteiden päivittämiseen määritellään riittävät resurssit. (Viestintävirasto 2016, 4.)

Laitevalmistajien tietoturvatiedotteita on hyvä noudattaa ja seurata jatkuvasti. Ilmoituksia uusista haavoittuvuuksista sekä tietoturva- ja tietosuojaloukkauksista otetaan vastaan organisaation sisältä, että sen ulkopuolelta. Ongelmiin ja uhkiin tulee reagoida välittömästi määritetyn tärkeysluokituksen mukaisesti, sekä toimintaa tulee pyrkiä parantamaan organisaation sisällä jatkuvasti (Viestintävirasto 2016, 4.). Erilaiset jo olemassa olevat tietoturvaratkaisut antavat valmiuksia organisaation toiminnan kehittämiselle, sekä turvallisuuden parantamiselle.

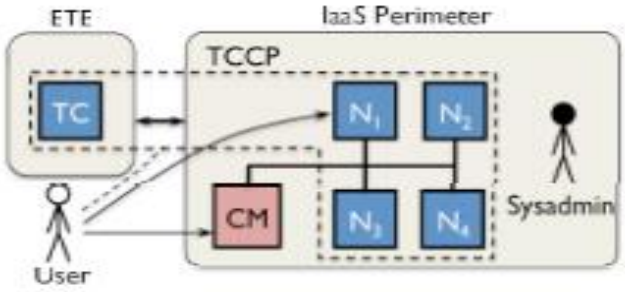
Esittelen seuraavissa kappaleissa luotetun alusta ratkaisun, yleisen tietoturvamallin sekä kaksi yritystä, jotka tarjoavat erilaisia tietoturvaratkaisuja pilvipalveluille. Opinnäytetyössä esiteltyjen tietoturvaratkaisujen sekä menetelmien on tarkoitus antaa palveluita hankkivalle organisaatiolle tai yritykselle alustavaa tietoa tarjolla olevista palveluista.

3.7.1 TCCP-alusta

TCCP eli Trusted Cloud Computing Platform tarjoaa suljetun hiekkalaatikkotestausympäristön, jotta IaaS-palvelun ohjelmistoa voidaan laajentaa ja kehittää. TCCP takaa luot-

tamuksellisen ja maailmanlaajuisen eheyden käyttäjien virtuaalikoneille, ja sallii käyttäjän määritellä etukäteen, valvooko IaaS näitä sovelluksia vai ei. Kuvassa 7 määritellään TCCP-alustan komponentit. Kuvaan 7 on merkattu luotettujen palvelinten (N) ja koordinaattorin (TC) välinen alusta, jossa palveluntarjoaja (CM) antaa palvelut käyttäjien saataville. Kuvassa 7 TC-alusta on luotetun ulkopuolisen yksikön ylläpitämä.

TCCP parantaa infrastruktuurin rakennetta ohjelmistossa ja mahdollistaa suljetun hiekkalaatikon semantiikan muuttamatta arkkitehtuuria. Potilastietoa siirrettäessä pilvipalveluihin koordinaattorin tulee pystyä tarjoamaan tietoturvallinen alusta käyttäjän tarvitsemalle palvelulle. Lähtökohtaisesti alustan on pystyttävä täyttämään tämänhetkiset ja myös tulevat viranomaisvaatimukset ja määrittelyt.



Kuva 7. TCCP-alustan komponentit (IJCA 2015,15).

Palvelualustaa voidaan väärinkäyttää pääsyoikeuksia omaavan järjestelmävalvojan kautta, jolloin oikeudet omaava valvoja voi asentaa haittaohjelman palveluun. IaaS palvelun tarjoajien kanssa kannattaa sopia, että palvelun alustan oikeudet ovat hajautettu, joten yhdellä käyttäjällä ei ole kaikkia oikeuksia muokata palveluita. Tässä voidaan hyödyntää NIST:in määrittelemää RBAC:ia (Role Based Access control) eli roolipohjaista pääsynhallintaa.

TCG (Trusted Computing Group) tarjoaa standardin alustan suunnitteluun, jossa TPM-siruun (Trusted Computing module) on tallennettu avainpari ja siru kytketty palvelimelle. Palvelimet yksilöidään käyttämällä TPM-sirun avainparia ja virtuaalikoneiden ajaminen palvelinten kautta turvallisesti varmistetaan koordinaattorilta (IJCA 2015, 15.). TCCP-alusta hyödyntää TPM-ominaisuuksia etätodennuksessa, jossa käynnistyksen aikana isäntä laskee ohjelmiston tiivistelistan käynnistysjärjestyksen, käynnistyslataajan ja toteuttaa sen ohjelmistoalustalla. Lista on varastoitu isäntä-moduulin sisälle turvallisesti. TCCP käyttää turvallisia kryptograafisia avaimia tunnistautumiseen eri osapuolien välillä. (IJCA 2015, 16.)

3.7.2 SecureCloud

Cloud Secure Alliancen SecureCloud on organisaation sisällä hallittavien usean eri pilvipalveluiden yhteen integroimiseen tarkoitettu tietoturvamalli. Tietoturvamalli noudattaa SOA-arkkitehtuurimallin vaatimuksia. Tietoturvamallin haasteena on mahdollistaa turvallinen tunnistautuminen, tiedonhallinta ja pääsynvalvonta. Käyttäjälle voidaan luoda riittävän vahva tunnistautuminen oman tunnuksen yhdistämisellä yleistunnukseen. Esimerkiksi ”yleistunnus + numerosarja”. Tietoturvavaatimusten tulee olla eri palveluiden välillä yhteensopivia. Tietoturvamalli tarjoaa integrointikomponentin turvalliseen viestintään eri tahojen välillä. Integrointikomponentti sisältää moduulin palveluidenominaisuuksien yhteensopivuuden tarkistamiseen, pääsynhallinnan valvomiseen ja turvallisuudenhallintaan. (CSA 2016.)

SecureCloud määrittelee tietoturvamallissa sertifiointijärjestelmän, jossa arviointi voidaan toteuttaa itsenäisesti tai kolmannen osapuolen toimesta. Sertifiointijärjestelmä määrittelee varmennusjärjestelmälle korkean riskin profiilit. Sertifiointijärjestelmä voi kuitenkin tuottaa haasteita organisaatiolle yksityisyyden ja tietosuojalakien noudattamisessa, sillä lait on määritelty maakohtaisesti. CSA painottaa OCF-viitekehyksen (Open Certification Framework) sekä STAR-rekisterin (Security Trust Assurance Registry) käyttöä pilvipalveluita hankittaessa. Järjestelmä on saanut tunnustusta turvallisuudesta ja sertifioinnista. Järjestelmä tarjoaa paljon työkaluja ja toimintatapoja pilvipalveluiden sidosryhmien vaatimuksille.

EU:ssa sovellettava SecureCloud määritelmä voidaan listata kymmeneen kiinnekohtaan, joita ovat tietosuoja muutokset, tavat joilla tietoa käsitellään, tiedonsiirto, tietojen tietosuoja, seuranta, henkilötietoja koskevat ilmoitukset, tietojen siirrettävyys, tietojen säilyttäminen, vastuullisuus yhteistyö ja lakisääteinen julkistaminen. SecureCloud noudattaa GDBR-säädöstä. (CSA 2016.)

3.7.3 SafeNet

SafeNet on yhdysvaltalainen tietoturvayritys, joka tarjoaa salausratkaisuja pilvipalveluille. Vuonna 1984 perustettu SafeNet on standardoitu ja tarjoaa kattavasti erilaisia salausmenetelmiä tietojen suojaamiseen. Yritys on kohdistanut palvelunsa erityisesti arkaluonteisten tietojen suojaamiseen ja salaamiseen pilvipalveluissa. SafeNetin tarjoamia

ratkaisuja ovat virtuaaliympäristön suojaus, tietokantojen suojaus, tiedostojen suojaaminen ja salausavainten suojaaminen. (SafeNet 2016.)

Virtuaaliympäristö pilvipalveluissa suojataan salaamalla koko virtuaalilaite sekä ohjelmistorajapinnat. Ylläpidon pääsyoikeudet suojattavaan tietoon estetään. Tietoturvatapahtuman aikana arkaluontoinen tieto voidaan salata. SafeNet noudattaa tietojen salauksessa HIPAA-lakia. Yrityksen käyttämät käyttöjärjestelmäalustat virtuaaliympäristössä ovat Amazon Web Services sekä WMware. Salausavainten suojaus noudattaa FIPS (Federal Information Processing Standards) tietoturvastandardia. Tietojen salaamiseen SafeNet käyttää AES (Advanced Encryption Standard) tekniikkaa ja palveluiden eheyden ja luottamuksellisuuden varmistamiseen sähköistä allekirjoitusta. (SafeNet 2016.)

3.7.4 Trend Micro

Japanilainen tietoturvayritys Trend Micro tarjoaa ohjelmistomoduuli pohjaista tietoturvaratkaisua pilvipalveluille. Ohjelmistomoduuli eli Runtime Agent varmistaa palvelun eheyden. Trend Micro hyödyntää AES-tekniikkaa palvelun salauksessa ja hallintatyökalussa. Trend Micro toimittaa palvelunsa asiakkaalle, joko yrityksen itsensä ylläpitämänä tai asiakkaan oman hallintapalvelimen kautta. (Trend Micro 2015.)

Hallintapalvelussa valvotaan lokitietoja, raportteja sekä salausavaimen hyväksymisprosessia. Tietoturvaratkaisun käyttämä salaus mahdollistaa virtuaalilaitteen työmuistin salauksen. Trend Micron pilvipalveluissa käyttäjä pystyy määrittelemään käytettävät palvelimet suojatun tiedon käsittelyyn. (Trend Micro 2015.)

Käyttäjät, toimittajat ja kolmannet osapuolet voidaan integroida yhteen pilvipalveluiden API rajapinnalla. WMware-tietoturvaratkaisu kattaa suojautumisen tietoturvauhkilta, pääsynvalvonnan, yksityisyyden, API-rajapinnan elinkaaren, organisoinnin, tuetut protokollat, korkean saatavuuden, API-rajapinnan hallinnan sekä tuetut standardit. Trend Micron tietoturvaratkaisu suojaa arkaluonteisen tiedon väärinkäytöltä kuten tiedon siirtämiseltä, tietovuodolta tai varkaudelta. (Trend Micro 2015.)

Avaintenhallintapolitiikka määrittelee kaikki palvelun ylläpitäjien oikeudet ja auttaa tietoaineiston kontrolloimisessa. Pilvipalvelun infrastruktuuria ylläpitävältä toimijalta voidaan evätä pääsy salattuun tietoon, kontrolloimalla fyysisten muistilaitteiden salausavaimia.

Trend Micro käyttää SecureCloud-viitekehystä lokien hallinnassa ja raportoinnissa. Palvelut tukevat FIPS-sertifiointia ja ovat muun muassa HIPAA- ja HITECH-standardoitu. (Trend Micro 2016.)

Trend Micro määrittelee tietoturvaratkaisut standardien mukaisesti ja tarjoaa käyttäjälle turvallisia menetelmiä arkaluontoisen tietoaineiston salaamiseen. Trend Micron ratkaisujen mukaan asiakas hallitsee itse salausavaimia, jolloin palveluiden tarjoajalla ei ole oikeuksia tiedon käyttöön. Palveluntarjoaja lupaa myös tietoaineiston täydellisen salauksen, jossa on keskitetty avaintenhallinta. Avaintenhallinta noudattaa yrityksen tietoturvapolitiikoita, ja hallinta on helposti automatisoitavissa.

Palvelimen luotettavuus ja eheys todennetaan automaattisesti avaimia pyydettäessä, jolloin varmistetaan, että käyttäjän identiteetti on oikea. Tietoaineisto ei ole haettavissa enää sen jälkeen, kun tieto on pilvipalvelusta poistettu. Politiikoita käytetään tietoaineiston valvomiseen, jolloin yrityksen on mahdollista tietää milloin, missä ja mitä tietoa on haettu. Pilvipalveluiden salaus on suunniteltu niin, ettei se vaikuta palvelun suorituskykyyn. (Trend Micro 2015.)

4 TIETOAINEISTON SALAUS

Verkkoyhteyttä hyödyntävässä ohjelmistossa on syytä varmistaa, että käytettävät yhteydet on salattu. Näin tiedon liikkuminen pilvipalveluiden ja tietokoneen välillä on turvallista. Ylläpitäjillä sekä kehittäjillä on suora pääsy palvelun toiminnallisuuteen, jolloin heillä on myös pääsy tietosisältöön. Palvelunhankkijan on syytä tehdä kaikille tietoaineistoon käsiksi pääseville turvallisuusselvitys sekä seurata alan standardeja.

Monet pilvipalvelut tarjoavat pääsynhallintaa ja palvelusopimuksessa voidaan määritellä ehdot tietojen käsittelyyn. Palvelunhankkijan on myös varmistettava, että arkaluontoisia tietoja käsittelevä henkilöstö on koulutettu ja toimii ohjeistetusti. Palvelua hankkivalla organisaatiolla tulee olla valmis, jatkuva, dokumentoitu riskienhallintaprosessi kaikille palvelua koskeville vaatimuksille, kuten komponenteille.

Pilvipalvelun fyysinen ympäristö täytyy suojata kulunvalvonnalla, jotta voidaan suojautua tiedon väärinkäytöltä ja minimoida riskit. Yleensä yksittäinen käyttäjä on suurin tietoturvauhka, jolloin väärinymmärrykset sekä vahingot voivat aiheuttaa suuriakin vahinkoja. Käyttäjäkoulutuksella ja ohjeistuksella pystytään välttämään monia virhetilanteita. Tietoaineisto voidaan salata käyttämällä erilaisia salaustekniikoita kuten RSA tai AES. Nämä salaustekniikat ovat ehdottomasti turvallisimpia, sillä salauksia on lähes mahdotonta purkaa ilman oikeaa salausavainta.

4.1 RSA-salaus

RSA-salausalgoritmi on yksi ensimmäisenä syntyneistä menetelmistä, jota käytetään julkisen avaimen salauksessa. Salaisen algoritmin kehitti englantilainen matemaatikko Clifford Cocks tiedusteluvirastolle vuonna 1973, sveitsiläisen matemaatikon Leonhard Eulerin kehittämästä lauseesta. Diffie ja Hellman esittivät julkisen avaimen salausmenetelmän vuonna 1976, josta Rivest, Shamir ja Adleman kehittivät RSA-salauksen vuonna 1977. MIT (Massachusetts Institute of Technology) patentoi RSA-algoritmin vuonna 1983, mutta menetti oikeudet patenttiin vuonna 2000, sillä RSA-menetelmä paljastettiin jo ennen patenttihakemusta. (Palola 2008, 2, RSA 2015.)

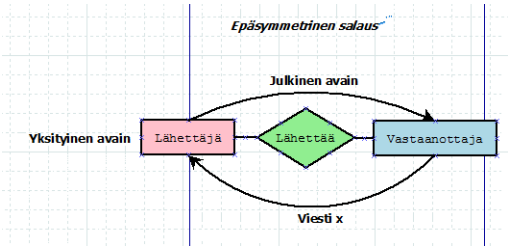
RSA-algoritmi perustuu yksisuuntaiseen modulaarifunktioon, jota on erittäin vaikea purkaa suurien alkulukujen takia. Alkuluvut ovat jaollisia vain itsellään tai 1:llä, joten tulon

tekijöihin jako on haastavaa. RSA:n julkisen avaimen salausjärjestelmä perustuu potenssinkorotusalgoritmiin ja RSA-menetelmä käyttää julkisia ja yksityisiä avaimia viestien salaamiseen. RSA-algoritmia käytetään myös viestien digitaaliseen allekirjoittamiseen tiivistefunktioiden avulla (Digitaalinen allekirjoitus 2015).

RSA-algoritmin suurien kokonaislukujen testaamisessa voidaan käyttää Miller-Rabinin testiä, joka laskee epädeterministisellä algoritmilla, millä todennäköisyydellä luku on alkuluku. Intialaiset Manindra Agrawal, Neeraj Kayal ja Nitin Saxena kehittivät deterministisen AKS-testin määrittämän, onko jokin luku alkuluku. AKS-testi voidaan suorittaa polynomisessa ajassa, mutta AKS-testi on silti hitaampi suorittaa kuin epädeterministinen Miller-Rabinin testi. (Palola 2008, 22.)

RSA-salausalgoritmin turvallisuus perustuu suurien alkulukujen tulon tekijöihin jakamiseen. RSA-menetelmään kohdistetut hyökkäykset suunnataan avaimeen, jolloin avaimen murtaminen teoriassa on yksinkertaista, mutta hidasta. RSA on turvallinen, jos salausavain on riittävän pitkä. Tietokoneiden laskentakapasiteetin kehittyessä avaimen pituutta täytyy kasvattaa, jotta RSA:n käyttö olisi turvallista. (Rinne 1994, 2.)

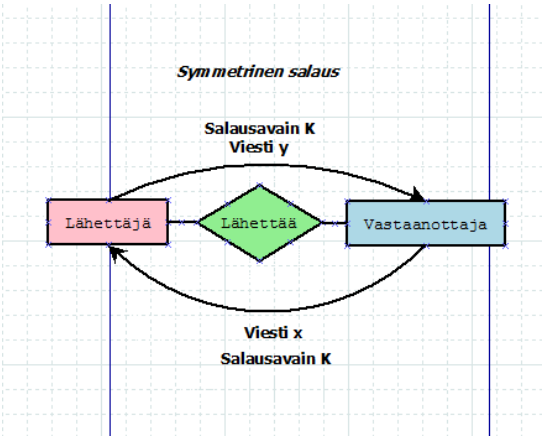
RSA:n viestien salaamismenetelmä perustuu julkisen ja yksityisen avaimen käyttöön. Salatut viestit luodaan julkisen tai yksityisen avaimen avulla, ja ne voidaan vastaavasti lukea käyttäen yksityistä tai julkista avainta. Viestin salaamisessa ja purkamisessa voidaan käyttää kahta eri menetelmää, joita kutsutaan epäsymmetriseksi ja symmetriseksi salaukseksi (RSA 2015). Epäsymmetriseksi salaukseksi kutsutaan menetelmää, jossa lähettäjä lähettää julkisen avaimen vastaanottajalle, mutta pitää yksityisen avaimen itsellään. Vastaanottajan on mahdollista lähettää salainen viesti lähettäjälle ja vain lähettäjä voi lukea viestin käyttäen yksityistä avaintaan. (Kuva 8.)



Kuva 8. Epäsymmetrinen salaus.

Lähettäjä voi myös julkaista julkisen avaimen, jolloin kuka tahansa voi lähettää salatun viestin lähettäjälle ja vain viestin vastaanottaja voi avata salauksen yksityisellä avaimellaan. (Julkisen avaimen salaus 2015.)

Symmetrisessä salauksessa lähettäjä ja vastaanottaja käyttävät viestin salaamisen ja purkamiseen samaa salausavainta. (Kuva 9.)



Kuva 9. Symmetrinen salaus.

Symmetriset salausalgoritmit jaetaan kahteen eri menetelmään. Ensimmäinen menetelmä on jonosalaus, jossa tietojono salataan lineaarisesti ja tieto generoidaan satunnaisesti. Toinen menetelmä on lohkosalaus, jossa määritellyn mittainen pala tietoa salataan. (Delfs & Knebl 2007, 32.)

RSA-salausalgoritmin suuret alkuluvut määritellään valitsemalla satunnainen suuri kokonaisluku ja testaamalla, onko se alkuluku. Kokonaisluku voidaan testata jakamalla, Miller-Rabinin testillä tai AKS-testillä. Alkulukutestien algoritmit perustuvat todennäköisyyksiin, eivätkä ne takaa oikeaa tulosta. Toistaiseksi ei ole kehitetty kaavaa testaamaan onko jokin luku alkuluku. (Palola 2008, 17–22.)

RSA-salauksen tekijöiden jakamiseen vaadittava aika kasvaa eksponentiaalisesti suhteessa tekijöihin jaettavan luvun kokoon. Ei voida kuitenkaan todistaa, etteikö olisi mahdollista jakaa luku tekijöihinsä tehokkaasti ja nopeasti algoritmin avulla (Rinne 1994, 2.) RSA-menetelmän murtaminen tapahtuu jakamalla julkisen avaimen yhteinen osa tekijöihin, jonka tuloksena saadaan tekijöihin jaetut alkuluvut. Alkulukujen perusteella voidaan laskea avaimen julkinen osa.

Lohkosalausmenetelmässä salattava tieto jaetaan osiin ja salataan yksitellen. Hyökkääjä pystyy erottamaan salatusta tiedosta lohkot, joilla on sama lähdeteksti. Lohkosalausta käytetään vain turvallisessa toimintamoodissa, jotta salattava tieto pysyy turvassa. Francois Morain on tutkinut suurten kokonaislukujen tekijöihin jakoa ja havainnut faktorointialgoritmin löytämisen epätodennäköiseksi (Moirain Francois 2015).

RSA on määritelty turvalliseksi algoritmiksi, jos salausavain on yli 1024–2048 bittiä. Tietokoneiden laskentakapasiteetti ei tule silti kuitenkaan kehittymään lähivuosikymmenien aikana niin nopeasti, että pystyttäisiin helposti murtamaan yli 1000-bittisiä RSA-avaimia (Taulukko 1.). (Ala-Korpela ym. 2007, 59–60.)

Taulukko 1. Tekijöihin jakamisen kesto avaimien eri pituuksille (RSA 2016).

Avaimen pituus (bittiä)	**Aika**
128 bittiä	n. 2 sekuntia
192 bittiä	16 sekuntia
256 bittiä	35 minuuttia
260 bittiä	1 tunti

RSA-algoritmin avulla voidaan määrittää viestin tiiviste, jonka viestin lähettäjä sekä vastaanottaja laskevat tiivistefunktion avulla. Tiiviste muodostetaan salaista avainta käyttäen ja vastaanottaja voi avata tiivisteen vain käyttämällä samaa avainta. Tiivistettä kutsutaan myös hajautusarvoksi. Hajautusarvon tarkoituksena on tiivistää tieto. Tiivistefunktio tuottaa viestistä lyhyen tiivistelmän, joka edustaa viestiä. On vaikeaa löytää viesti, jolla olisi samanlainen tiiviste, sillä tiivisteen pituus on yleisesti 128–160 bittiä, oli viesti miten pitkä tahansa. Tiivisteen eli hajautusarvon avulla voidaan vertailla alkuperäistä tietoa vertailemalla tiivisteitä. (Tiiviste 2015.)

Tiivisteitä voidaan käyttää myös sähköpostin tai tekstitiedoston muuttumattomuuden varmistamiseen. Yksikin muutos jälkikäteen rikkoo tiivisteen, esimerkiksi virukset voidaan huomata muuttuneesta tiivisteestä. Tiivisteihin voi myös lisätä takaovia, jolloin hyökkääjän on helpompi päästä sähköpostiin tai tiedostoon käsiksi. (Järvinen 2012, 122.)

4.2 AES-salaus

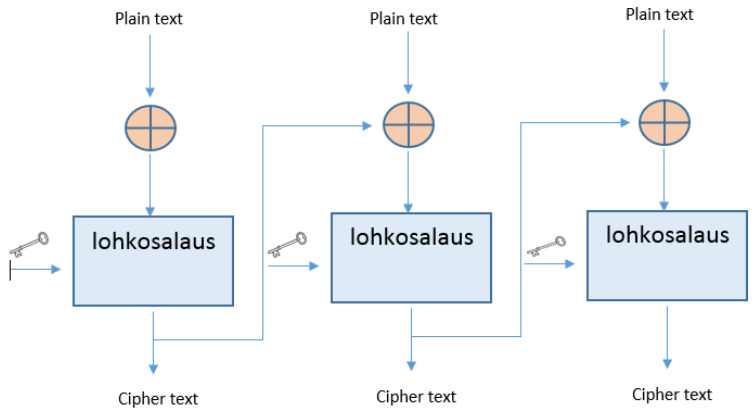
AES eli Advanced Encryption Standard on Rijndael-salaukseen perustuva salausstandardi. Salauksen on kehittänyt Joan Daemen ja Vincent Rijmen vuonna 2001. Salausstandardi on yhdysvaltalaisen NISTin standardoima ja seuraaja DES-salaukselle (Data Encryption Standard). DES-salausta ei kuitenkaan voida enää pitää turvallisena, sillä 64-bittinen salaus murrettiin brute force -menetelmällä alle vuorokaudessa. (AES 2016.)

AES-salausta käytetään henkilötietojen, ohjelmistojen, organisaatioiden ja verkkoliikenteen salaamiseen. AES käyttää symmetristä lohkosalaus menetelmää tietojen salaamiseen ja purkamiseen. Tietojen salaaminen ja purkaminen tapahtuu kierroksien avulla. Kierrosten lukumäärä riippuu käytettyjen avainten pituudesta (Taulukko 2.).

Taulukko 2. Kierrosten lukumäärän suhde avainten pituuteen.

Avaimen pituus	Kierrokset
128 bittiä	10
192 bittiä	12
256 bittiä	14

Kaikki muut paitsi viimeinen kierros sisältävät neljä tasoa, joita ovat “sub bytes”, “shift rows”, “mix columns” ja “add round key”. Jokainen syötteen tavu korvataan korvaustaulukosta valitulla tavulla. Kuvassa 10 on esitetty AES-salauksen rakenne yksinkertaistettuna.



Kuva 10. AES-salauksen rakenne.

Seuraavana AES-salauksessa tapahtuu rivin vaihto, jossa tavu ottaa oikealla olevan tavun paikan. Rivin vaihdon jälkeen tulee sarakkeiden sekoitus ja viimeisenä vaiheena AES-salauksessa on avainten laajennus ja uusien avainten luominen. AES-salauksen rakenteessa kuvattu salattava tieto (plain text) muuttuu kierrosten jälkeen salatuksi tiedoksi (cipher text) (ETN 2014). AES-salaus on luotettava lohkosalausmenetelmä, ja se on nopeampi kuin muut menetelmät.

4.3 SSL/TLS-tekniikka

SSL/TLS-tekniikkaa käytetään tietoliikenteen salaamiseen. Sähköisten palvelujen ja käyttäjien välinen viestintä on suojattu SSL/TLS-menetelmällä, joka on yleinen verkkopalveluissa käytetty salausmenetelmä. TLS eli Transport Layer Security salausprotokollaa käytetään tietoliikenteen suojaamiseen IP-verkkojen yli. SSL ja TLS ovat käytännössä sama asia, mutta TLS-tekniikka on uudempi versio SSL-protokollasta. SSL/TLS-protokolla on esitelty myös aikaisemmin OSI-mallin kuljetuskerroksessa.

Suojatun yhteyden tunnistaa selaimen osoiterivillä näkyvästä HTTPS-tunnuksesta. Yhteyden ollessa salainen useat selaimet näyttävät suljetun lukon kuvaketta selaimen osoiterivillä. Tietokoneen ei pitäisi tallenna salattuja sivuja välimuistiin. SSL-tekniikassa selain tarkistaa palvelun henkilöllisyyden lähettämällä palvelimelle todistuspyynnön henkilöllisyydestä. Palvelin vastaa todistukseen varmenteella. Selain tarkistaa varmenteen muuttumattomuuden digitaalisella allekirjoituksella. Valmis varmenne sijoitetaan palvelimelle ja salaus kytketään päälle. (Järvinen 2012, 59–60, Singh 1999, 399–402.)

Pankit ovat tietoturvarikosten tyypillisimpiä kohteita. Verkkopankit käyttävät SSL-salaustekniikkaa, mutta hakkerit ovat pystyneet murtautumaan verkkopankkeihin virusten avulla. Vuonna 2012 hakkerit varastivat EuroGrabber-viruksen avulla Euroopan verkkopankeista 36 miljoonaa euroa. (Haasio 2013,100–101.)

4.4 Salauksen luominen palveluun

Pilvipalveluiden tulee käyttää alan standardien vaatimustenmukaisia salaavia siirtoprotokollia, kuten työssä esiteltyjä SSL/TLS-protokollia. Salausprotokollia käytetään tiedon siirtämiseen palvelinten, laitteiden ja käyttäjien laitteiden välillä. Salausvaihtoehtoina voidaan käyttää eri salauksia riippuen siitä, minkälaista salausta tietojen käyttö edellyttää. Liikkuvat tiedot voidaan salata SSL/TLS-tekniikka käyttäen ja tallennettavat tiedot AES- tai RSA-salausta käyttäen.

Monet pilvipalvelutarjoajat tarjoavat luotettavan standardien mukaisen salauksen käyttäjän palveluille. Tämä helpottaa yrityksien palveluiden siirtämistä pilveen. Kuitenkin pilvipalvelua hankittaessa tulee käyttäjän ymmärtää riskit arkaluontoisten tietojen käytölle ja säilytykselle pilvipalveluissa. Kun käyttäjä ja pilvipalveluiden tarjoaja noudattavat yhteisiä vaatimuksia ja standardeja, voidaan pilvipalvelut ottaa turvallisesti käyttöön.

Avainten sekä varmenteiden sulkemiseen tai mitätöintiin voidaan käyttää CRL-sulkulistaa (Certificate Revocation List). Äkillinen avainten sulkeminen voidaan suorittaa silloin, kun avaimet ovat paljastuneet tai niitä käytetään väärin. Yleisesti uudet avaimet luodaan vanhojen avainten mitätöinnin jälkeen. (VAHTI 2009.)

4.5 Palveluun tunnistautuminen

Tutkimuksessa on hyödynnetty KATAKRIa palveluun tunnistaumisessa. Organisaatiolla tulee olla tarkat turvatoimet tiedon suojaustasoon, muotoon, määrään, sijoitustilaan ja luokitteluun suhteutettuna arvioituihin uhkiin, sekä käytössä henkilökohtaiset käyttäjätunnisteet. Kaikki käyttäjät, jotka käyttävät palvelua tulee tunnistaa ja todentaa yksilöidyllä tunnisteella. Todentamisessa ja tunnistamisessa on käytettävä turvallista tekniikoita. Useasti epäonnistuneen kirjautumisen tulee aiheuttaa tunnuksien lukkiutumisen. Yhteiskäyttötunnuksille tulee olla sovitut ja dokumentoidut hallintakäytännöt, mutta niitä tulee välttää. (KATAKRI 2015.)

Salasanatodennuksessa salasanan tulee täyttää turvallisuusvaatimukset. Salasana pakotetaan vaihtamaan vähintään kolmen kuukauden välein. Käyttäjän tunnistukseen vaaditaan vahva, vähintään kahteen tekijään perustuva käyttäjätunnistus. Päätelaitteiden tunnistaminen teknisesti tapahtuu ennen palveluun tai verkkoon pääsemistä. Verkkoon pääseminen voidaan rajata suppeaksi, fyysisten turvallisuuden menetelmien avulla. Esimerkiksi lukitsemalla verkkokaapeli, niin ettei sitä saa irrotettua. (KATAKRI 2015.)

Nämä suojaustavat tulee kuitenkin harkita organisaatio kohtaisesti palvelun käytössä. Käyttäjätunnistus ja päätelaitteen tunnistaminen voidaan toteuttaa rajaamalla tietojärjestelmään pääsy fyysisesti tiukasti suojatulta alueelta, jossa käytetään pääsynvalvonnassa vahvaa tunnistautumista, kuten esimerkiksi sirullista kulkukorttia ja tunnuslukua yhdessä. Käyttäjän tunnistaminen voidaan suorittaa käyttäjätunnus-salasana parilla tietojärjestelmässä, todennusmenetelmä tulee kuitenkin olla tarkasti suojattu. (KATAKRI 2015.)

Verkon yli lähetettävässä todennuksessa tunnistamistiedot tulee olla salatussa muodossa, jotta sisään kirjautuessa ei paljasteta ylimääräistä tietoa. Todennusmenetelmän tulee suojata uudelleenlähetyshyökkäyksiä vastaan. Käyttäjätilin yksilöiminen voidaan suorittaa myös siten, että kahden henkilön tulee osallistua salasanan todentamiseen.

Todennuksen järjestämiseen suositellaan muun muassa kahdennettujen palvelinten hyödyntämistä. (KATAKRI 2015.)

Kun käyttäjänhallintaa halutaan toteuttaa luotettavasti, tulee palveluun kuulua rekisteröinti sekä rekisteröidyn käyttäjän tunnistaminen. Käyttäjän tulee käyttää palvelussa pääsääntöisesti palvelun käyttöön tarkoitettua tietokonetta, jos tietokone on muiden käyttäjien käytössä, käyttäjän on poistuttava kaikista ohjelmista ja palveluista, ennen kuin lähtee pois tietokoneelta. Selaimen välimuisti on tyhjennettävä palvelun käytön jälkeen. Sivuhistoriatiedot tyhjentää tarvittaessa. Palveluun tunnistautumisessa kannattaa hyödyntää IAM-pääsynhallintamenetelmää (Identity Access Management). (KATAKRI 2015.)

4.6 Tietoaineiston kontrollointi

Tietoaineiston kontrollointia on tutkittu hyödyntämällä KATAKRIa. Käyttöoikeuksien hallinnointi kuuluu osaksi tietoaineiston kontrollointia. Hallinnoinnin tärkein tehtävä on jakaa käyttöoikeuksia henkilöille ja estää tiedon väärinkäyttö. Jokaisella käyttäjällä on käytössä rooliin pohjautuva näkymä ohjelmasta ja se toimii omalla virtuaalisella tai fyysisellä palvelimella. Organisaatiossa kaikkien tulee noudattaa samoja tietoturvapolitiikoita ja käyttöpolitiikoita sekä toimia niiden asettamien vaatimusten mukaan. Organisaatiolla tulee myös olla tarvittava asiantuntemus tietoturvallisuuden varmistamiseksi. Poikkeamista tehdyt havainnot tulee sisällyttää dokumentointiin. (KATAKRI 2015.)

Henkilöstön turvallisuuskouluttaminen tulee myös huomioida palvelun käyttöönotossa. Turvallisuuskoulutuksen sisällön dokumentoiminen kannattaa sisällyttää käyttöönottoon heti alusta lähtien. Tietojen monitasoinen suojaaminen on huomioitava koko tiedon säilytyksen elinkaaren ajan. Monitasoinen suojaaminen tarkoittaa joukkoa toisiaan täydentäviä turvatoimia. Suojaamisessa otetaan huomioon tietojen suojaustaso, tiedon määrä, sekä rakennusten ympäristö ja rakenne. Pääsynhallintaa voidaan kontrolloida kameravalvonnan, turvavalaistuksen, murtohälytysjärjestelmän ja säilytystilan avulla. Turva-alue tulee määritellä selkeästi ja suojata rajat. Alueelle on pääsy ilman saattajaa vain sellaisella henkilöllä, jolla on liiketoiminnallinen tarve kulkea alueella. (KATAKRI 2015.)

Palvelun käyttöönotossa tulee huomioida vain vaatimusten mukaiset ja olennaiset laitteet ja toiminnot. Järjestelmät sekä sovellukset kovennetaan ja asennus sisältää vain sellaiset toiminnot ja palvelut, jotka täyttävät toimintavaatimukset turvallisuuden varmistamiseksi. Kovennusten tulee pohjautua yleisiin hyviin suosituksiin ja kovennusohjeisiin

ja estää ajettavan koodin oletusarvoisen suorittamisen. Verkon aktiivilaitteiden salasanojen tulee noudattaa organisaation salasanapolitiikkaa. Laitteet ovat rajattu vain tarpeellisien verkkopalveluiden käyttöön ja ohjelmistoihin on asennettu turvapäivitykset. Istuntojen aikakatkaisut ovat hyvä menetelmä hallintayhteyksien kontrollointiin. (KATAKRI 2015.)

Tarjottavat palvelut kannattaa rajata sekä sovelluksiin tulee järjestää tarvittava verkkoliikenteen valvonta. Palveluiden turvaamiseksi on olemassa erilaisia ratkaisuja, joista yleisiin suojauskäytäntö on palomuuriratkaisu. Asetuksien muuttaminen on estetty valtuuttamattomilta käyttäjiltä. Asetuksiin pääsy tulee suojata salasanalla ja tarpeettomat portit sekä palvelut poistetaan käytöstä. Järjestelmät sekä ohjelmistojen päivitykset tulee hakea ja noutaa vain luotettavilta palveluntarjoajilta. Automatisoiduille prosesseille tulee määritellä vain tarvittavat tiedot ja valtuudet suorittaa toimintoja. (KATAKRI 2015.)

Kaikkiin järjestelmiin tulee asentaa haittaohjelmien torjuntaohjelmistot. Ohjelmistojen täytyy olla toimintakykyisiä ja tuottaa havainnoistaan lokitietoja sekä hälytyksiä. Hälytyksiä seurataan jatkuvasti ja niihin reagoidaan. Haittaohjelmatunnisteita kuuluu päivittää säännöllisesti sekä käyttäjiä tulee ohjeistaa haittaohjelmista. Verkko kannattaa myös segmentoida, jolloin sovellusten ja tietoaineiston kontrolloiminen on helpompaa ja nopeampaa. Lokitiedot kannattaa sisällyttää keskitettyihin lokipalvelimiin, jolloin pystytään varmistamaan lokitietojen tarvittava turvalinen säilytys, lokitietojen rakenteen muutos, tai tietomurto tapauksissa tahallinen lokitietojen muuttaminen. (KATAKRI 2015.)

Tiedon poistaminen tai hävittäminen tulee tapahtua kontrolloidusti valtuutetun henkilön toimesta. Tietojen poistaminen tapahtuu erillisellä ohjelmistolla, joka yli kirjoittaa poistettavan tiedoston levypinnan. Varmistaakseen tiedon hävittämisen kiintolevyn voi murskata tai sulattaa. Mikäli tiedostoja tarvitsee hävittää vain osittain, voidaan esimerkiksi roskakorin sisältö hävittää ylikirjoitusmenetelmällä. Ylikirjoitus voidaan automatisoida toteuttamaan koneen sammutuksen tai järjestelmän käynnistyksen yhteydessä. (KATAKRI 2015.)

5 YHTEENVETO JA POHDINTA

Tämän opinnäytetyön tutkimuksen tuloksena voidaan todeta, että arkaluontoisten tietojen, kuten potilastietojen siirtäminen ja käyttö hybridipilvipalveluissa, on turvallista, mikäli noudattaa alan standardeja sekä säädöksiä Suomen lainsäädännön mukaisesti. Opinnäytetyössä tutkittiin erilaisia tietoturvaratkaisuja sekä salausmenetelmiä, jotta saataisiin mahdollisimman kattava kuva tarjolla olevista palveluista. Lisäksi työ antaa kattavan ohjeistuksen palveluiden hankintaan, jolloin täytyy muistaa ottaa huomioon paljon erilaisia asioita. Työtä lukiessa on kuitenkin hyvä huomioida, ettei opinnäytetyötä ainoastaan voida soveltaa palveluiden hankintaan, sillä tekniikat ja standardit on esitelty suppeasti.

Tekniikan kannalta palveluntarjoajalla on merkittävä rooli palvelua hankittaessa. Kun lääkinnällisestä laitteesta siirretään tietoa pilvipalveluihin, tulee toimijan kiinnittää huomiota siihen, että tietoa siirretään turvallisesti laitteesta palveluun. Opinnäytetyön tavoitteena oli saada aikaan toimiva ohjeistus arkaluonteisten tietojen siirtämiseen pilvipalveluihin. Pilvipalvelumalleja tutkittaessa päädyttiin hybridipilvipalveluun, koska se tarjoaa parhaimmat edellytykset kustannustehokkaaseen ja palveluiltaan skaalautuvaan palvelumalliin. Tämän lisäksi tutkittiin myös pilvipalveluiden tietoturvaa ja siihen käytettäviä alan standardeja sekä arkkitehtuurimalleja, jotka soveltuvat hybridipilvipalveluiden käyttöön. Standardit ja lait antavat erittäin kattavan kuvan siitä, miten palvelun tietoturva kannattaa toteuttaa.

Tutkimuksessa havaittiin myös liiketoiminnallisia etuja sellaisille organisaatioille, jotka ovat tietoisia pilvipalveluiden muuttuvista standardeista sekä pystyvät noudattamaan näitä vaatimuksia. Tietoturvastandardit muotoutuvat koko ajan paremmiksi sekä palveluntarjoajien, että käyttäjien tulee seurata säädösten ja standardien muuttumista aktiivisesti. Lisäksi palveluntarjoajien erilaiset tietoturvapalvelut tietojen kontrollointiin sekä salaukseen kehittyvät jatkuvasti. Siksi olisikin hyvä tarkistaa tarjolla olevat markkinat ennen kuin ostaa pilvipalveluita.

Pilvipalveluiden hankintaan on hyvä varata tarvittavat resurssit ja osaavat asiantuntijat. Pilvipalveluiden käyttöönotossa käyttäjän tulee ymmärtää monia erilaisia yksityiskohtia. Kun hankinnasta on tehty kunnollinen suunnitelma ja vaatimustenmukaisuus on varmistettu, niin pilvipalvelun käyttöönotto on erittäin helppoa. Palvelussa olevien potilastietojen salaaminen ja pääsynhallinta sekä tietoaineistojen kontrollointi asetetaan keskeisimmiksi osiksi tiedon suojaamisessa.

Opinnäytetyön haasteina oli aiheen rajaus, sillä aihe oli erittäin laaja ja moniulotteinen. Tutkimuksen haasteena oli myös löytää materiaalia potilastietojen siirtämisestä pilvipalveluihin, sillä materiaalia potilastietojen siirtämisestä on erittäin vähän saatavilla. Kuitenkin palveluiden siirtyessä koko ajan enemmän pilveen tulee myös arkaluontoisen tiedon siirtämisestä pilvipalveluun ajankohtaista. Pilvipalveluiden tietoturvalla on tällöin valtavasti potentiaalia kasvavilla markkinoilla. Kun tietoa aletaan siirtää pilveen, myös tietoturva monipuolistuu ja tulee tarjoamaan enemmän ja parempia ratkaisuja tietojen suojaamiseksi.

Työn tavoitteet ja vaatimukset muuttuivat opinnäytetyön aikana, sillä pilottivaihe ei käynnistynyt RAMP-projektissa ajallaan ja aihealueesta oli rajattava materiaalia pois. Kuitenkin työn peruselementit saatiin pidettyä kasassa ja kuvattua tarpeeksi yksityiskohtaisesti. Opinnäytetyön tarkoituksena oli antaa kattava ja selkeä kuva pilvipalveluiden tietoturvasta ja tiedon turvallisesta siirrosta laitteesta palveluun.

LÄHTEET

AES 2016. Advanced Encryption Standard. Viitattu 4.5.2016 https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

Ala-Korpela, M.; Inkinen, S. & Suna, T. 2007. Kyborgin käsikirja. Helsinki: Finn Lectura Oy, 2007.

Authorize.Net 2015. Merchant Web Services API. Customer Information Manager (CIM) SOAP Guide. Viitattu 16.3.2016 http://www.authorize.net/content/dam/authorize/documents/CIM_SOAP_guide.pdf.

CSA 2009. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Viitattu 16.3.2016 https://cloudsecurityalliance.org/csaguide.pdf.

CSA 2016. Current Cloud Certification Challenges Ahead and Proposed Solutions. Viitattu 6.6.2016 https://csacongress.org/wp-content/uploads/2016/05/Daniele-Catteddu-Certification-Challenges-and-Proposed-Solutions.pdf.

Delfs, H.; & Knebl, H. 2007. Symmetric-key encryption. *Introduction to cryptography: principles and applications*. Springer 2007.

Digitaalinen Allekirjoitus 2015. Wikipedia. Viitattu 4.2.2016 https://fi.wikipedia.org/wiki/Digitaalinen_allekirjoitus.

ETN 2014. Elektroniikka tietoliikenne nanotekniikka. AES-salausta tehokkaammin. Viitattu 4.5.2016 http://etn.fi/index.php?option=com_content&view=article&id=2218:aes-salausta-tehokkaammin&catid=26&Itemid=140.

Google 2016. Viitattu 6.7.2016 https://cloud.google.com/products/.

Haasio, A. 2013. Netin pimeä puoli. Helsinki: Suomalaisen Kirjallisuuden Seura.

Hankosalo A. 2014. Tietosuoja pilvipalveluissa. Opinnäytetyö. Tietojenkäsittelyn koulutusohjelma. HAAGA-HELIA ammattikorkeakoulu. Viitattu 18.4.2016 https://www.theseus.fi/bitstream/handle/10024/76185/AnneHankosalo-TietosuojaPilvipalveluissa.pdf?sequence=1.

Health Insurance Portability and Accountability Act 2016. Viitattu 8.6.2016 https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act.

Heino, P. 2010. Pilvipalvelut. Hämeenlinna: Talentum Media Oy.

Henkilötietolaki 22.4.1999/523.

IBM 2006. TCP/IP Tutorial and Technical Overview. Viitattu 1.6.2016 https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf.

ICO 2016. Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now. Viitattu 3.6.2016 https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf.

IJCA 2015. Trusted Cloud Computing Platform into Infrastructure as a Service Layer to Improve Confidentiality and Integrity of VMs. Viitattu 2.6.2016 http://www.ijcaonline.org/research/volume131/number7/yoganand-2015-ijca-907361.pdf.

ITIL 2014. IT service management and cloud computing. Viitattu 4.5.2016 https://www.axelos.com/CMSPages/GetFile.aspx?guid=ede50958-eccb-46e1-b982-7816100d8fb9.

ITU 1994. ITU-T: TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU. Viitattu 17.3.2016 http://www.itu.int/rec/T-REC-X.200-199407-I.

ITU 2014. SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Cloud computing security – Overview of cloud computing security. Security framework for cloud computing. Viitattu 1.6.2016 https://www.itu.int/rec/T-REC-X.1601-201510-I/en.

Julkisen avaimen salaus. 2015. Wikipedia. Viitattu 4.2.2016 https://fi.wikipedia.org/wiki/Julkisen_avaimen_salaus.

Järvinen, P. 2012. Arjen Tietoturva − vinkit & ratkaisut. Jyväskylä: Docendo Oy.

Järvinen, P. 2010. Yksityisyys: Turvaa digitaalinen kotirauhasi. Jyväskylä: WSOYpro.

KATAKRI 2015. Puolustusministeriö. Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 4.6.2016 http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf.

Kunnat.net 2016. Viitattu 6.7.2016 http://www.kunnat.net/fi/tietopankit/uutisia/2016/Sivut/EUn-tietosuoja-asetus-muuttaa-henkilotietojen-kasittelya.aspx.

Kyberturvallisuuskeskus 2014. Pilvipalveluiden tietoturva. Viestintävirasto. Viitattu 18.4.2016 https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf.

Limnell J. & Majewski K. & Salminen M. 2014. Kyberturvallisuus. Jyväskylä: Docendo Oy.

Microsoft 2015. HIPAA ja HITECH-laki. Viitattu 6.6.2016 https://www.microsoft.com/fi-fi/TrustCenter/Compliance/HIPAA.

Morain Francois 2015. Wikipedia. Viitattu 4.2.2016 https//de.wikipedia.org/wiki/Fran%C3%A7ois_Morain.

NIST 2016. NIST Cloud Computing Program. Viitattu 15.3.2016 http://www.nist.gov/itl/cloud/.

NIST 2011. The NIST Definition of Cloud Computing. Viitattu 16.3.2016 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

OASIS 2016. OASIS SOA Reference Model (SOA-RM) TC. Viitattu 17.3.2016 https://www.oasis-open.org/committees/soa-rm/faq.php.

OASIS 2012. Reference Architecture Foundation for Service Oriented Architecture Version 1.0. Viitattu 17.3.2016 http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/cs01/soa-ra-v1.0-cs01.pdf.

Palola, J. 2008. RSA-Salausalgoritmi ja alkuluvut. Pro gradu–tutkielma. Tietojenkäsittelytieteiden laitos. Tietojenkäsittelyoppi. Tampereen Yliopisto. Viitattu 4.2.2016 https://tampub.uta.fi/bitstream/handle/10024/78940/gradu02474.pdf?sequence=1.

Rinne, T. 1994. RSA:n turvallisuus. Viitattu 4.2.2016 https://timo.rinne.ws/teleseminaari/subsection2_4_1_2.html.

RSA 2015. Wikipedia. Viitattu 4.2.2016 https://fi.wikipedia.org/wiki/RSA.

RSA 2016. Wikipedia. Viitattu 4.2.2016 https://en.wikipedia.org/wiki/RSA_(cryptosystem).

SafeNet 2016. Gemalto. Viitattu 1.6.2016 https://safenet.gemalto.com/cloud-data-security/.

Salo I. 2012. Hyötyä pilvipalveluista. Jyväskylä: Docendo Oy.

Seppälä M. 2011. Pilvisovelluskehitys Google App Engine –pilvisovellusalustalla. Diplomityö. Lappeenrannan teknillinen yliopisto. Viitattu 4.4.2016 https://www.doria.fi/bitstream/handle/10024/69812/nbnfi-fe201106131742.pdf?sequence=3.

Singh, S. 1999. Koodikirja. Suomentaja Karjalainen, H. Jyväskylä: Gummerus kirjapaino.

Suomi 2015. Tietosuoja. Viitattu 18.4.2016 https://www.suomi.fi/suomifi/suomi/asioi_verkossa/tietosuoja/index.html.

Tietoyhteiskuntakaari 7.11.2014/917. Viitattu 21.4.2016 http://www.finlex.fi/fi/laki/ajantasa/2014/20140917.

Tietosuoja 2010. Henkilötietojen käsittelyn ulkoistaminen, yhteiset tietojärjestelmät, verkottuminen ja niihin liittyvät sopimukset. Viitattu 18.4.2016 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfppPP8x/Henkilotietojen_kasittelyn_ulkoistaminen_yhteiset_tietojarjestelmat_verkottuminen_ja_niihin_liittyvat_sopimukset.pdf.

Tietojen salaaminen 2016. Yksityisyydensuoja. Viitattu 4.5.2016 https://www.yksityisyydensuoja.fi/tietojen-salaaminen.

Tiiviste 2015. Wikipedia. Viitattu 4.2.2016 https://fi.wikipedia.org/wiki/Tiiviste_(tietotekniikka).

Trend Micro 2015. Integrated Data Loss Prevention. Viitattu 7.6.2016 http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ds_integrated-data-loss-prevention.pdf.

Trend Micro 2015. Instant-On Security for the Cloud. Viitattu 4.6.2016 http://www.trendmicro.com/cloud-content/us/pdfs/sb_trend_micro_cloud_security.pdf.

Trend Micro 2016. SMART PROTECTION SUITES. Viitattu 6.6.2016 http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ds_smart-protection-complete.pdf.

VAHTI 2009. Viitattu 28.6.2016 https://www.vahtiohje.fi/web/guest/406.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681. Viitattu 21.4.2016 http://www.finlex.fi/fi/laki/ajantasa/2010/20100681.

Viestintävirasto 2016. Terveydenhuoltoalan kyberuhkia 1/2016. Viitattu 17.5.2016 https://www.viestintavirasto.fi/attachments/tietoturva/Terveydenhuoltoalan_kyberuhkia.pdf.

W3C 2013. Semantic Web Activity Statement. Viitattu 17.3.2016 https://www.w3.org/2001/sw/Activity.

W3C 2012. Web Services Internationalization (WS-I18N). Viitattu 17.3.2016 https://www.w3.org/TR/2012/NOTE-ws-i18n-20120522/.